Jc973 U.S. PTO 10/033034 12/27/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年１２月２８日

出 願 番 号
Application Number: 特願２０００－４０３４７２

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ４月 ６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０２５９９０

【書類名】　特許願
【整理番号】　0001076230
【提出日】　平成12年12月28日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　神谷　成樹
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　山下　雅美
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100067736
　【弁理士】
　【氏名又は名称】　小池　晃
【選任した代理人】
　【識別番号】　100086335
　【弁理士】
　【氏名又は名称】　田村　榮一
【選任した代理人】
　【識別番号】　100096677
　【弁理士】
　【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　配信方法及び配信システム

【特許請求の範囲】

【請求項１】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の複数の鍵情報を生成する処理と、生成された複数の鍵情報をディジタルコンテンツとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを用いて配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、複数の配信経路を通じて配信を受けた複数の鍵情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタ

ルコンテンツの元データをスクランブル処理して出力する処理とを実行させ、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項２】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされるこ

とを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項３】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項４】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテ

ンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた部分鍵又はその発生情報と、第１の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項５】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第１の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第２の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第１の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理と

を実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項６】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第１の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第２の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツ

に付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項７】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項８】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテ

ンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第１の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項９】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第２の暗号鍵によって上記第１の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、上記第２の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して

出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１０】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第２の暗号鍵によって上記第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、上記第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残

りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１１】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって暗号化された上記第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、上記第２の

暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた合わせ鍵の一部と、第２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１２】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システム

と、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第２の暗号鍵によって上記第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、上記第２の暗号鍵を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サ

ーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１３】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第２の暗号鍵によって上記第１の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、上記第２の暗号鍵を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除された

ディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１４】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第２の暗号鍵によって上記第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、上記第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サ

ーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１５】　特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタル

コンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって暗号化された上記第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、上記第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でス

クランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項１６】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムであって、

上記復号サーバは、配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除部と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化部と、復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備え、

上記出力装置は、上記受信サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、上記スクランブル解除部でスクランブルが解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツを所定の出力形態で再生する信号処理部とを備える

ことを特徴とする電子配信システムにおける下流側システム。

【請求項１７】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバであって、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除部と、

ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化部と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする復号サーバ。

【請求項１８】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとしての回路装置であって、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除部と、

ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化部と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする回路装置。

【請求項１９】　コンピュータを、特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとして、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除処理と、

ディジタルコンテンツに付属する再生条件が満たされることを条件にスクラン

ブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化処理と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理と

を実行させるためのプログラムを記録した記録媒体。

【請求項２０】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバであって、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化部と、

復元されたディジタルコンテンツの唯一の出力先であって、スクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする復号サーバ。

【請求項２１】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとしての回路装置であって、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、デ

ィジタルコンテンツの元データを復元する復号化部と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする回路装置。

【請求項２２】　コンピュータを、特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとして、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除処理と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化処理と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理と

を実行させるためのプログラムが記録された記録媒体。

【請求項２３】　配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバであって、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部を備える

ことを特徴とする復号サーバ。

【請求項２４】　配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバとしての回路装置であって、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部を備える

ことを特徴とする回路装置。

【請求項２５】　コンピュータを、配信を受けたディジタルコンテンツに施さ

れている暗号処理を解除する復号サーバとして、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理を実行させるプログラムを記録する記録媒体。

【請求項２６】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置であって、

上記受信サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、

上記スクランブル解除部でスクランブルが解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツを所定の出力形態で再生する信号処理部とを備える

ことを特徴とする出力装置。

【請求項２７】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置としての回路装置であって、

上記受信サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部を備える

ことを特徴とする回路装置。

【請求項２８】　コンピュータを、特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置として、

上記受信サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除処理

を実行させるプログラムを記録した記録媒体。

【請求項２９】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおける信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルコンテンツに施された暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、上記処理で暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とする下流側システムにおける信号処理方法。

【請求項３０】　特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバにおける信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルコンテンツに施された暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコン

テンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行する

ことを特徴とする復号サーバにおける信号処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はディジタルコンテンツの配信方法及び配信システムに関する。また、本発明は、ディジタルコンテンツの配信方法及び配信システムの実現に必要な要素技術に関する。

【０００２】

【従来の技術】

ディジタル技術の進展に伴い、あらゆるディジタルコンテンツ（文字データ（例えば、記号、図形）、オーディオデータ（例えば、音声、音楽）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータその他のディジタルデータ）がネットワークや記録媒体を通じて配信されようとしている。

【０００３】

【発明が解決しようとする課題】

一方、ディジタルコンテンツは完全な複製物を容易に作成できるため、不正行為（例えば、不正復号再生、不正複製、横流し）が行われると、非常に大きな損害が生じるものと予測される。このため、不正行為からコンテンツ提供者（コンテンツ制作者や配信事業者）を保護する仕組み作りが急がれている。特に、制作に膨大な費用と人手を要し、資産価値の高いコンテンツ（例えば、映画）に関しては、不正行為によって莫大な損害が生じるため、不正行為が著しく困難な仕組み作りが求められる。

【０００４】

しかし、防御能力が高いものは多大な設備投資を必要としたり、設備投資が比較的少なくて済むものは防御能力に問題がある等、コンテンツ提供者と受け手の

双方が納得できるような仕組みは確立されていないのが現状である。

【０００５】

例えば、不正行為に対する耐性を高く保ち続けたり、より再現性の高い出力技術が現れた場合には適宜最新の技術を導入できることが望ましいが、現在提案されているビジネスモデルでは受け手側に必要な機能を全て出力装置内に設ける構成を採るため、技術寿命の短いものに合わせて出力装置自体の買い替えが必要となる。しかし、出力装置の短期間での買い替えを前提とするビジネスモデルでは、受け手側の理解を得ることができない。またその結果として、陳腐化した技術の置き換えが進み難く、ディジタルコンテンツが不正行為にあう危険性が高まるという弊害がある。

【０００６】

このため、資産価値の高いコンテンツの提供がコンテンツ制作者に認められなかったり、ビジネスモデル自体が受け手側に受け入れられず、システムの運用を開始できない等の問題が生じている。

【０００７】

本願明細書は以上の課題を考慮し、ディジタルコンテンツの配信段階から最終出力段階に至るまで不正行為が極めて難しく、しかも合理的な対価によって長期にわたって高い防御機能を維持できる配信方法及び当該方法を適用したシステム並びにそれらを実現する要素技術について提案する。

【０００８】

【課題を解決するための手段】

かかる課題を解決するため以下の手段を提案する。

【０００９】

（１）本願明細書で想定する配信モデル

以下の各手段では後述する処理を実行する上流側システムと下流側システムとで構成される配信モデルを想定する。

【００１０】

上流側システムが、ディジタルコンテンツ毎に固有の暗号処理を施し、すなわちディジタルコンテンツ毎に固有の暗号鍵でディジタルコンテンツを暗号化し、

放送形式又は記録媒体の形態で下流側システムに配信を行う。このようにコンテンツに固有の暗号鍵を用いることにより、不正行為が行われてもその被害がコンテンツ単位でしか生じないようにする。

【００１１】

また、上流側システムは、ディジタルコンテンツの暗号化に使用した暗号鍵の配信に際し、基本的に以下の２種類の方法のいずれかによって作成した配信先に固有の複数の鍵情報を、ディジタルコンテンツとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを通じて対応する下流側システムに配信する。すなわち、鍵情報を複数の経路を通じて配信することにより、いずれかの経路を通じて配信される鍵情報が盗まれた場合でも、他の全ての鍵情報が盗まれない限り被害の発生を防止できる。なお配信される鍵情報は、暗号鍵そのものだけでなく、その発生情報（例えば、乱数）でもよい。また鍵情報は、暗号鍵を分割した合わせ鍵や部分鍵でもよい。

【００１２】

因みに上述の２種類の方法は、

１）暗号鍵を配信先毎に固有の分割パターンで分割し、一組の部分鍵を生成する方法

２）配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でディジタルコンテンツの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号したものを生成する方法

の２つである。

【００１３】

ここでの配信先毎に固有の分割パターンや配信先毎に固有の異なる暗号鍵は、配信者毎に普遍的に割り当てられている場合もあれば、コンテンツ毎にその都度割り当てられる場合もある。勿論、不正行為対策の観点からは後者が望ましい。

【００１４】

一方、下流側システムは、複数の鍵情報から復元した暗号鍵でディジタルコンテンツに施されている暗号処理を解除する処理と、これにスクランブル処理を施

す処理を復号サーバで実行し、スクランブル処理の施されたディジタルコンテンツを出力装置に対して出力する。

【００１５】

このように暗号処理の復号機能を出力装置とは別に設けるようにしたことにより、受け手側にとって設備の更新負担が少なくて済むシステム構成とできる。すなわち、配信システムの運用開始後に暗号方式の変更を行う場合にも、復号サーバだけを更新すればよく、暗号処理の復号とは関係のない出力装置については性能に支障のない限りそのまま使用できるようになる。同様に、出力装置をより性能の高いものに置き換える場合でも何らの問題のない復号サーバについてはそのまま使用できるようになる。かかる仕組みは長期的な運用コストを低減する上で効果的である。

【００１６】

もっとも、単に復号機能と出力装置とを分離したのでは不正行為に対して極めて無防備な配信モデルとなってしまうが、復号サーバと出力装置との間を流れるのはスクランブル処理されたディジタルコンテンツであるので、復号サーバと出力装置の間でディジタルコンテンツを不正複製することはできないようになっている。

【００１７】

なお、復号サーバや出力装置においても不正行為の起こり得ない仕組みを採用する。例えば、正規の手続き以外では復号サーバや出力サーバの筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。また、復号サーバにおいて実行される特定の処理機能を集積回路化して処理の過程で現れる暗号鍵や生のディジタルコンテンツが取り出されないようにする仕組みを採用する。ここで正規の手続きとしては、例えば開封する資格を有する者のみが保持する電子的な鍵や物理的な鍵を使用することが考えられる。また、不正に開封する行為としては、例えば筐体を破壊することが考えられる。

【００１８】

（２）配信モデルを実現する代表的な手段

以下、配信モデルを実現する代表的な手段について説明する。ここでの配信モ

デルは、前述のように上流側システムと下流側システムとで構成される配信システムを前提とする。また以下では、配信モデル全体からみた配信方法について説明する。

【００１９】

なお、各手段の上流側システムで実行される各処理は、上流側システムを構成する制作者システム及び配信者システムのいずれかで行われる。処理機能どのように振り分けるかはビジネス上の選択による。従って、制作者システムと配信者システムの具体的なハードウェア構成やソフトウェア構成は種々のものが考えられる。例えば、ディジタルコンテンツを暗号化するまでの処理と各配信先に応じた複数の鍵情報を生成する処理については制作者システムで行われるようにすると、暗号鍵（マスター鍵）を知り得るのはコンテンツ制作者のみとなるため、コンテンツ制作者にとって秘匿性を保持し易い処理方法となる。

【００２０】

以下の手段では、電子透かしについて言及していないが、不正行為の防止や流出経路の特定の観点からはディジタルコンテンツを暗号化する前に、固有の電子透かしを入れておくことが望ましい。

【００２１】

また、暗号化されたディジタルコンテンツの配信に際し、配信事業者や伝送網の管理者が別途他の暗号処理を施すことは自由である。また、鍵情報を配信する場合にも、実際にはディジタル証明書等によって相手先が真正な配信先であることを確認した上で相手方の公開鍵で鍵情報を暗号化しておくことが安全を期する上で望ましい。

【００２２】

なお以下の手段では、分割処理によって暗号鍵から直接得られる鍵を「合わせ鍵」と、合わせ鍵を更に分割することで得られる鍵を「部分鍵」というものとする。もっとも、いずれの鍵も暗号鍵の一部分である点では同じである。また以下の手段では、暗号鍵を暗号化するのに使用する鍵を「多重鍵」というものとする。

【００２３】

また各手段において鍵情報を配信する場合には、鍵情報の伝送網に、ディジタルコンテンツの伝送網と物理的に同じものを用いることも可能である。ただし、その場合にはディジタルコンテンツと鍵情報を同時刻に配信することはせず、それぞれの配信時間帯をずらし、実際上、別経路で配信するのと同様の状態で配信を行うことが望ましい。これは、ディジタルコンテンツと鍵情報を同一の伝送網を通じて同時配信すると、１回の不正行為でディジタルコンテンツと鍵情報の一部を同時に入手できるため、その分、ディジタルコンテンツに施されている暗号が解除される危険性が高まるためである。

【００２４】

（２－１）第１の手段

第１の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。なお、上流側システムは、ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとで構成される複合システムである。また、下流側システムは、ディジタルコンテンツに施されている暗号処理を解除する復号サーバと、ディジタルコンテンツを所定の出力形態で再生する出力装置とで構成される複合システムである。これは他の手段でも同様である。

【００２５】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００２６】

また、下流側システムの復号サーバが、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号

鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００２７】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００２８】

第１の手段は要するに、ディジタルコンテンツの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部を伝送網を通じて配信し、残りを記録媒体の形態で配信する配信方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルコンテンツにスクランブル処理を施し出力装置に出力する再生方式とを組み合わせたものである。

【００２９】

ここで、合わせ鍵の配信に使用する記録媒体には、磁気読み取り方式の媒体（例えば、磁気テープ、フロッピーディスク、磁気カード）、光学読み取り方式の媒体（例えば、ＣＤ－ＲＯＭ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ）、半導体メモリ（メモリカード（矩形型、正方形型など形状は問わない。）、ＩＣカード）その他が考えられる。当該記録媒体の配信には、郵便制度や宅配制度を使用する。現行の制度では、秘匿性の観点から書留郵便の使用を想定する。この配信用の記録媒体についての記載は以下の各手段についても共通である。

【００３０】

また、合わせ鍵の配信に使用する伝送網は、ディジタルコンテンツを伝送網を介して伝送する場合、基本的にはディジタルコンテンツと別のものを使用する。ただし、両者を同じ伝送網を使って配信することも可能である。なお、両者を同じ伝送網を通じて伝送する場合には、合わせ鍵の伝送とディジタルコンテンツの伝送とは時間的に別の時間帯に行うことが不正行為に対する対抗上望ましい。これらの記載も、後述する各手段に現れる部分鍵や多重鍵の配信に共通する。

【００３１】

また、復号サーバで生成するスクランブル鍵とスクランブル解除鍵は、同じディジタルコンテンツについては同じであってもよいし、暗号処理を解除する毎に固有の鍵を発生するようにしてもよい。不正行為に対する対策としては後者の方が望ましい。

【００３２】

また、出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。

【００３３】

ここで、出力装置における所定の出力形態には、ディジタルコンテンツが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またディジタルコンテンツが例えばオーディオデータであれば、スピーカを通じての再生が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に２つの出力が行われる。

【００３４】

なお、この第１の手段では信号処理の観点から説明しているが、これらの処理機能を備えるハードウェア構成によって実現することも可能であるし、同様の機能をソフトウェア処理として実現することも可能である。後述する他の手段についても同様である。この場合、ハードウェアやソフトウェア（コンピュータに該当処理を実行させるプログラムを記録した記録媒体）は上流側システムと下流側システムのそれぞれについて用意する。ハードウェアには、復号サーバや出力装

置といった完成品の他、インタフェースボードや半導体集積回路等といった構成部品（請求項における回路装置）が考えられる。

【００３５】

かかる手段を用いることにより、たとえ複数の経路で配信される鍵情報のうちいずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルコンテンツとは別に配信されるため、生のディジタルコンテンツが復号化される事態を確実に回避できる。

【００３６】

また、暗号処理が解除されたディジタルコンテンツにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。すなわち、十分な対不正行為能力と経済性とを兼ね備えた配信モデルを提供できる。

【００３７】

（２－２）第２の手段

第２の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００３８】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残

りの合わせ鍵又はその発生情報を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００３９】

また、下流側システムの復号サーバが、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００４０】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００４１】

第２の手段は要するに、ディジタルコンテンツの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部はそのまま第１の伝送網を通じて配信するものの、残る合わせ鍵については更に所定の分割規則で分割し、生成された一組の部分鍵の一部を第２の伝送網を通じて配信し、残りは記録媒体の形態で配信する方式を採用するものであり、この点で第１の手段と異なっている。

【００４２】

すなわち、鍵情報の配信を２つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現する点で異なるものである。

【００４３】

ここで、合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でもよいし、各配信先に固有の規則でもよいし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でもよい。他の手段においても同様である。

【００４４】

かかる手段を用いる場合には、第１の手段よりも更に鍵情報の配信経路が増えるため、伝送経路上での不正行為により高い耐性を有する配信モデルを提供できる。

【００４５】

なおここでは、合わせ鍵の一部を更に分割して配信用の鍵情報を生成しているがこれに代え、多重鍵で暗号化する方式を採用することもできる。かかる変形例は、同様の仕組みを採用する他の手段についても同様である。

【００４６】

（２－３）第３の手段

第３の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００４７】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又は

その発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００４８】

また、下流側システムの復号サーバが、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００４９】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００５０】

第３の手段は要するに、第２の手段では第２の伝送網を介して配信した合わせ鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を１つの伝送網と２つの記録媒体とで実現するものである。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００５１】

かかる手段も、第１の手段に加えて更に鍵情報の配信経路が増えるため、より不正行為に対する安全性の高い配信モデルを提供できる。また、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対抗策を採り易いという効果が期待できる。

【００５２】

（２－４）第４の手段

第４の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００５３】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第１の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第２の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００５４】

また、下流側システムの復号サーバが、第１の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００５５】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００５６】

第４の手段は要するに、第１の手段では記録媒体を使用して配信した合わせ鍵を伝送網を用いて配信する方式を採用するものである。すなわち、鍵情報の配信を２つの伝送網を用いて実現するものである。ここでの配信も、異なる２つの伝送網を用いて配信する場合と、同一の伝送網を用いながら異なる時点に鍵情報を配信することで等価的に２つの伝送網を用いた配信とする場合が考えられる。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはディジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【００５７】

かかる手段を用いることにより、全ての鍵情報を即時性に優れた伝送網を通じて配信することになるので、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をディジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたディジタルコンテンツを盗んでも生のディジタルコンテンツを復号化することはできない。

【００５８】

（２－５）第５の手段

第５の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００５９】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配

信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００６０】

また、下流側システムの復号サーバが、第１の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第２の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００６１】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００６２】

第５の手段は要するに、第１の手段では伝送網を介して配信した合わせ鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を２つとも記録媒体の形態で実現するものである。この場合も、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り

方式については同じでも、異なっても構わない。

【００６３】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くディジタルコンテンツの盗難の起こり難いという効果が期待できる。

【００６４】

（２－６）第６の手段

第６の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００６５】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００６６】

また、下流側システムの復号サーバが、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツ

に施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００６７】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００６８】

第６の手段は要するに、第２の手段では記録媒体を用いて配信していた部分鍵を伝送網を介して配信する方式を採用するものである。すなわち、３つの鍵情報の全てを伝送網を通じて配信するものである。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはディジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【００６９】

この手段の場合、全ての鍵情報を即時性に優れた伝送網を通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合に比して鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をディジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたディジタルコンテンツを盗んでも生のディジタルコンテンツを復号化することはできない。

【００７０】

（２－７）第７の手段

第７の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００７１】

上流側システムが、各ディジタルコンテンツに固有の暗号鍵を発生する処理と、ディジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００７２】

また、下流側システムの復号サーバが、第１の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００７３】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを

所定の出力形態で再生する処理とを実行するものを提案する。

【００７４】

第７の手段は要するに、第３の手段では伝送媒体を介して配信していた部分鍵を記録媒体を用いて配信する方式を採用するものである。すなわち、３つの鍵情報の全てを記録媒体を用いて配信するものである。この場合も、３つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００７５】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くディジタルコンテンツの盗難の起こり難いという効果が期待できる。

【００７６】

（２－８）第８の手段

第８の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００７７】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００７８】

また、下流側システムの復号サーバが、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタ

ルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００７９】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００８０】

第８の手段は要するに、配信先（下流側システム）毎に固有の第２の暗号鍵であって、暗号化するディジタルコンテンツに固有なもので暗号化した第１の暗号鍵を伝送網を通じて配信し、その暗号化に使用した第２の暗号鍵を記録媒体の形態で配信する方式を採用するものである。この手段は、配信される鍵情報の発生の仕方が第１の手段と異なるだけで、配信の仕方自体は第１の手段の場合と同じである。

【００８１】

かかる手段を用いることにより、たとえ複数の経路で配信される鍵情報のうちいずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルコンテンツとは別に配信されるため、生のディジタルコンテンツが復号化さ

れる事態を確実に回避できる。

【００８２】

また記録媒体として配信される第２の暗号鍵が盗まれた場合でも当該鍵はディジタルコンテンツに固有なものであるため、同じ配信者にそれ以後配信されるディジタルコンテンツの解除には使用することができず、被害の継続的発生を確実に防止できる。

【００８３】

（２－９）第９の手段

第９の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００８４】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００８５】

また、下流側システムの復号サーバが、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所

的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００８６】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００８７】

第９の手段は要するに、第８の手段では記録媒体の形態で配信した配信先に固有の暗号鍵を所定の分割規則で分割し、生成された一組の合わせ鍵の一部を伝送網を通じて配信し、残りは記録媒体の形態で配信する方式を採用するものである。すなわち、第９の手段では、配信先に固有の暗号鍵がそのままの状態で配信されるのを回避するものである。

【００８８】

なお当該手段における配信は、全体的にみると、鍵情報の伝送を２つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するものである。

【００８９】

ここで、配信先に固有の暗号鍵から一組の合わせ鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でもよいし、各配信先に固有の規則でもよいし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でもよい。

【００９０】

かかる手段では、第８の手段と異なり、各配信先に固有の暗号鍵がそのままの状態で（記録媒体の中ではあるが）配信されないため、記録媒体の盗難だけでは多重鍵を入手することはできず、その分、ディジタルコンテンツの不正復号を困

難にできる。

【００９１】

（２－１０）第１０の手段

第１０の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００９２】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００９３】

また、下流側システムの復号サーバが、伝送網を通じて配信を受けた合わせ鍵の一部と、第２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタ

ルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【００９４】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【００９５】

第１０の手段は要するに、第９の手段では第１の伝送網を介して配信されていたディジタルコンテンツ用の暗号鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を１つの伝送網と２つの記録媒体とで実現するものである。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっているものでも構わない。

【００９６】

かかる手段の場合には、暗号化された暗号鍵が記録媒体を通じて配信される分、当該鍵を伝送網を通じて配信する場合に比して盗難の早期発見を可能とでき、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【００９７】

（２－１１）第１１の手段

第１１の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００９８】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を第２の伝

送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【００９９】

また、下流側システムの復号サーバが、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【０１００】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【０１０１】

第１１の手段は要するに、第８の手段では記録媒体を用いて配信した第２の暗号鍵を伝送網を通じて配信する方式を採用するものである。すなわち、鍵情報の配信を２つの伝送網を用いて実現するものである。この手段は、配信される鍵情報の発生の仕方が第４の手段と異なるだけで、配信の仕方自体は第４の手段の場合と同じである。

【０１０２】

かかる手段を用いることにより、たとえ複数の経路で配信される鍵情報のうち

いずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルコンテンツとは別に配信されるため、生のディジタルコンテンツが復号化される事態を確実に回避できる。

【０１０３】

（２－１２）第１２の手段

第１２の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【０１０４】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【０１０５】

また、下流側システムの復号サーバが、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化

処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【０１０６】

下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【０１０７】

第１２の手段は要するに、第８の手段では伝送媒体を介して配信した暗号化済みの第１の暗号鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を２つとも記録媒体の形態で実現するものである。この手段は、配信される鍵情報の発生の仕方が第５の手段と異なるだけで、配信の仕方自体は第５の手段の場合と同じである。

【０１０８】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くディジタルコンテンツの盗難の起こり難いという効果が期待できる。

【０１０９】

（２－１３）第１３の手段

第１３の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【０１１０】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号

化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【０１１１】

また、下流側システムの復号サーバが、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【０１１２】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【０１１３】

第１３の手段は要するに、第９の手段では記録媒体を用いて配信していた部分鍵を伝送網を介して配信する方式を採用するものである。すなわち、３つの鍵情

報の全てを伝送網を通じて配信するものである。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはディジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【０１１４】

この手段の場合、全ての鍵情報を即時性に優れた伝送網を通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合に比して鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をディジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたディジタルコンテンツを盗んでも生のディジタルコンテンツを復号化することはできない。

【０１１５】

（２－１４）第１４の手段

第１４の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【０１１６】

上流側システムが、各ディジタルコンテンツに固有の第１の暗号鍵を発生する処理と、ディジタルコンテンツを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行するものを提案する。

【０１１７】

また、下流側システムの復号サーバが、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルコンテンツに施されている暗号処理を解除する処理と、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【０１１８】

また、下流側システムの出力装置が、復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【０１１９】

第１４の手段は要するに、第１０の手段では伝送媒体を介して配信していた部分鍵を記録媒体を用いて配信する方式を採用するものである。すなわち、３つの鍵情報の全てを記録媒体を用いて配信するものである。この場合も、３つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっているものでも構わない。

【０１２０】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くディジタルコンテンツの盗難の起こり難いという効果が期待できる。

【０１２１】

【発明の実施の形態】

（１）ビジネスモデル

（１－１）一般例

図１に本願明細書が想定するビジネスモデルの一般構成例を示す。このビジネスモデルは、ディジタルコンテンツの配信者と、ディジタルコンテンツの受け手である特定者とから構成される。配信者はコンテンツ制作会社１と電子配信事業者２で構成される。特定者６及び７は個人宅や事業者で構成される。

【０１２２】

なお、コンテンツ制作会社内のシステムと電子配信事業者内のシステムとが配信システムにおける上流側システムを構成し、特定者内のシステムが配信システムにおける下流側システムを構成する。

【０１２３】

配信対象に想定するディジタルコンテンツは、文字データ（例えば、記号、図形）、オーディオデータ（例えば、音声、音楽）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータ、その他のディジタルデータがある。

【０１２４】

一般に、ディジタルコンテンツの配信には、伝送帯域が広く大容量のデータを配信するのに適した高速配信用ネットワーク３を想定する（図１）。ただし、ＣＤ－ＲＯＭやＤＶＤその他の記録媒体による形態での配信を排除するものではない。高速配信用ネットワーク３には、放送衛星や光ファイバその他の広帯域伝送網を使用する。これらは少なくとも下り方向について大容量の伝送が可能なものを使用する。もっとも、上り方向への伝送も可能な双方向伝送網を用いてもよい。

【０１２５】

高速配信用ネットワーク３には、図２に示したようなデータ構造のデータ８が配信される。ここで、図１のデータ８には鍵の絵８Ａを表しているが、これはネ

ットワーク提供事業者が独自に掛けた鍵を表している。

【０１２６】

勿論、ここでの鍵は暗号処理のことである。これらの鍵が掛けられないこともある。ディジタルコンテンツの不正行為に対する安全性を最優先するコンテンツ制作会社１や電子配信事業者２は、ネットワーク上でも独自にデータに暗号処理を施すネットワーク事業者を選択するであろうし、その中でもより安全性の高い暗号処理を実行するネットワーク事業者を選択するものと考えられる。

【０１２７】

破線で囲まれた中身の部分が電子配信事業者２から出力されるデータに相当する。図２の場合、当該データには、データ又はファイルの格納情報を示すファイルアロケーションテーブル（ＦＡＴ：File Allocation Table）８Ｂと、ディジタルコンテンツの使用条件（配信先、配信先毎の再生可能期間及び再生回数その他の条件）を含む業務データ８Ｃと、映像データ８Ｄと、音声データ８Ｅとが格納されている。

【０１２８】

これら各データに掛けられている鍵の絵は、コンテンツ制作者１又は電子配信事業者２のいずれかのシステムにおいて、又はその双方のシステムにおいて各コンテンツに固有の鍵が掛けられていることを表している。

【０１２９】

映像データ８Ｄには、異なる符号化復号化方式（コーデック）で符号化された複数種類のディジタル映像コンテンツが格納される。図１では、３種類のコーデックに対応するディジタルコンテンツが格納されている状態を表している。例えば、ＭＰＥＧ（Moving Picture Experts Group）、Ｗａｖｅｌｅｔその他がある。

【０１３０】

このようにディジタル映像コンテンツを複数種類のコーディック方式で符号化し配信するのは、特定者側のシステム構成に自由度をもたせるためである。すなわち、特定者側に単一コーデックのシステム構成を強制するのではなく、各自に都合のよいコーディックを選択可能とするためである。

【０１３１】

音声データ８Ｅについても同様である。図２の場合、２種類のコーデック方式で符号化されたデータが格納されている。例えば、ＭＰＥＧその他がある。

【０１３２】

図１の場合、特定者Ａと表した個人宅が必要とするデータは、映像コーデック１と音声コーデック１であるため、それらが配信を受けたデータの中からＦＡＴの情報を基に選択的に受信される又は再生される。同様に、特定者Ｂと表した事業者が必要とするデータは、映像コーデック２と音声コーデック２であるため、それらが配信を受けたデータの中からＦＡＴの情報を基に選択的に受信される又は再生される。

【０１３３】

以上が高速配信用ネットワーク３を介して配信を受けるディジタルコンテンツについての説明である。次に、当該ディジタルコンテンツに施されている条件付きアクセス処理、すなわち暗号処理を解除するのに必要な暗号鍵の配信経路について説明する。図１における暗号鍵の配信経路は、広域ネットワーク（伝送媒体）４と記録媒体５の２つである。共通鍵を復元するのに少なくとも２種類の鍵情報を必要とする場合において、その一部を広域ネットワーク４を介して電子的に配信し、残る一部を記録媒体５を通じて物理的に配信する方式を採用する。

【０１３４】

なお、ここでの広域ネットワーク４は双方向通信が可能な伝送網を想定している。例えば、公衆網（例えば、インターネット網、ＡＴＭ網、パケット通信網）や専用線網が考えられる。また、記録媒体５は前述の課題を解決するための手段にて述べたように、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他を想定する。その配信に郵便制度や宅配制度を利用することも前述の通りである。

【０１３５】

ここで、ディジタルコンテンツに掛けられている暗号処理を解除するのに必要な鍵は全ての配信先について共通であるが、各配信先に個別に配信される鍵情報は、図１における特定者Ａの鍵情報と特定者Ｂの鍵情報のように、各配信者毎に

固有なものを想定する。これはある特定者宛てに配信された全ての鍵情報を入手しなければ、ディジタルコンテンツに掛けられている鍵を復元できないようにするためである。このような仕組みを採用することで、このビジネスモデルは、全ての鍵情報の入手がより困難なもの又は全ての鍵情報を入手するまでに時間を要するものとしている。なお時間がかかる分、鍵情報の盗難が発見された後、暗号鍵を変更する等の対策が可能となる。

【０１３６】

ところで、ディジタルコンテンツに掛けられる暗号鍵と各配信先に配信される鍵情報のそれぞれとしては、いずれも配信対象であるディジタルコンテンツに固有なものを使用する。これは、全ての鍵情報が不正に入手されてディジタルコンテンツの復号に成功されたとしても被害を当該ディジタルコンテンツのみに限定するためである。

【０１３７】

また、基本的に鍵情報の配信経路は、図１に示すように、ネットワークと記録媒体というように媒体を異にするもの想定する。これは以下の理由による。まず、ネットワークでの配信は即時に実行できるという利点を有するが、その一方で鍵情報が盗難されても発見が難しいという欠点がある。これに対し、記録媒体での配信は特定者が入手するまでに時間を要するという欠点を有するものの、鍵情報の盗難を物理的に確認することができ、盗難を発見し易いという利点がある。

【０１３８】

そこで、本願明細書で想定する多くのビジネスモデルでは、ネットワークを介しての配信と、記録媒体による物理的な配信との組み合わせを想定する。もっとも以上は一般的な理由によるものであり、ネットワークを使った配信でも不正行為のおそれがない場合や困難な場合には、全ての鍵情報をネットワークを介して配信すればよい。また、鍵情報の配信からディジタルコンテンツの配信までに期間的な余裕がある場合には、鍵情報の全てを記録媒体を使用して配信することもできる。

【０１３９】

因みに、ディジタルコンテンツの暗号処理に使用する暗号技術については技術

的な制約はなく、出願当時知られている各種の技術は勿論のこと将来現れるであろう各種の技術についても適用できる。暗号方式を問わないため技術的な寿命の影響を受け難いビジネスモデルとできる。また、常に運用当時最高の技術を選択できるため、その分、不正行為に強いビジネスモデルとできる。

【０１４０】

また図１において広域ネットワーク４と記録媒体５との２つの経路を通じて配信される鍵情報は、課題を解決するための手段において説明したように、配信先毎に固有の分割パターンで分割された一組の合わせ鍵（部分鍵）の組、又は、配信先毎に発生された固有の多重鍵で暗号化された暗号鍵と多重鍵の組を一般には想定する。

【０１４１】

（１－２）具体例

図３に、具体的なビジネスモデル例を示す。これは映画コンテンツを電子的に配信するビジネスモデルについてのものである。この種のビジネスモデルは従来からその実現に向け各種のビジネスモデル案が提供されているが、映画コンテンツの事業者と配信を受ける劇場側の双方から未だ納得を得られておらず、実用に至ったものはない。そこで、本願明細書の配信モデルを適用することを考える。

【０１４２】

このビジネスモデルの場合、図１のコンテンツ制作会社１は映画製作会社に変わり、ディジタルコンテンツの配信を受ける特定者は劇場Ａ、Ｂに変わる。なお図３の場合、映画コンテンツに特有な構成として、映画製作会社１から提供されるフィルム画像を電子画像に変換する工程（テレシネ工程：Film to Video Conversion）ａを表している。また図では区別していないが、劇場Ａ、Ｂは大規模な映画館、小規模な映画館、いわゆるシネコンと呼ばれる映画館が想定される。

【０１４３】

（２）配信システム例

上述のビジネスモデルを実現する配信システムの機能ブロック構成例を示す。なお各システム例は、課題を解決するための手段で説明した第１～第１４の各手段に対応する。

【０１４４】

（２－１）第１のシステム例

図４に、上述のビジネスモデルを実現するための第１のシステム例を示す。当該システムは上流側システムと下流側システムとで構成される。上流側システムは、コンテンツ制作会社１のシステムと電子配信事業者２のシステムの複合システムでなる。一方、下流側システムはディジタルコンテンツの配信を受ける特定者毎に固有のシステムでなる。

【０１４５】

（２－１－１）システム構成

図４の場合、上流側システムは、コンテンツサーバ１１と、コンテンツ符号化部１２と、暗号化部１３と、送出サーバ１４と、コンテンツ管理サーバ１５と、鍵発生部１６と、配信先管理サーバ１７と、合わせ鍵生成部１８と、書込部１９とから構成される。

【０１４６】

図４では、上流側システムにおけるこれらの各構成要素がいずれの事業者内システムに設けられるかをあえて明示していないが、これは各構成要素を上流側システムと下流側システムとでどのように配分するかはビジネス上の選択となるためである。なお各構成要素の配分の仕方は、他のシステム例についても共通する事項であるため、後段の「各システムで想定される運用形態」の項で別途説明する。

【０１４７】

一方、下流側システムは、受信サーバ３１と、読取部３２と、復号サーバ３３と、出力装置３４（デスクランブル部３４Ａ）とから構成される。このうち、復号サーバ３３は、更に復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）と、スクランブル制御部３６と、出力ログ管理部３７とで構成される。

【０１４８】

なお、これらの各構成要素はそれぞれ専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１４９】

また図中、太線で示す矢印は伝送容量の大きい伝送路を表しており、細線で示す矢印は伝送容量の比較的小さい伝送路を表している。もっとも現時点で想定されるシステム構成であり、伝送容量が大きいか小さいかは相対的なものである。また現時点では細線の矢印で示す合わせ鍵の配信経路も伝送容量の大きいものとしてもよい。

【０１５０】

（２－１－２）各機能部の構成

まず、上流側システムを構成する各機能部を説明する。コンテンツサーバ１１は、記録媒体（図４では磁気テープ）や伝送路を通じて提供を受けたディジタルコンテンツの蓄積を主な機能とする装置である。このため大容量のストレージ装置を備える。なお当該サーバはコンピュータ構成を採る。

【０１５１】

すなわち、当該サーバは、制御機能と演算機能を実現する処理装置と、信号処理の実行に必要なデータを記憶する記憶装置と、外部からデータやプログラム及びコマンドを入力する入力装置と、処理結果を外部に出力する出力装置とを備える構成を採る。

【０１５２】

コンテンツ符号化部１２は、ディジタルコンテンツの圧縮符号化その他の符号化処理を主な機能とする装置である。例えば、ＭＰＥＧ変換やＷａｖｅｌｅｔ変換その他の符号化処理が実行される。なお、符号化処理は一般に１種類だけが行われるのではなく、運用時に広く採用されている複数の符号化処理が行われる。この結果、１つのディジタルコンテンツに対して複数の符号化処理データが生成される。なお音声や画像データに透かし情報を埋め込む処理は、例えばコンテンツサーバ１１とコンテンツ符号化部１２との間で実行される。このコンテンツ符号化部１２は、専用のハードウェアを用いて構成してもよいし、当該ハードウェアと同等の機能を実現させるプログラムがインストールされているコンピュータのソフトウェア上の処置として実現してもよい。

【０１５３】

暗号化部１３は、鍵発生部１６からコンテンツに固有の暗号鍵の提供を受け、当該暗号鍵を用いてコンテンツ符号化処理の終了したディジタルコンテンツに暗号処理を施す装置である。ここで使用する暗号方式は運用時に広く採用されているものを用いればよい。

【０１５４】

例えば、ＤＥＳ（Data Encryption Standard）、ＦＥＡＬ（Fast Data Encipherment Algorithm）その他の暗号処理が実行される。ここでの暗号処理は、業務データとコンテンツデータのそれぞれについて個別に実行される。参考までに言及すると、コンテンツデータについての暗号処理は、コンテンツ符号化部１２で生成された各符号化データ毎に実行される。

【０１５５】

なお暗号化部１３も、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。

【０１５６】

送出サーバ１４は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルコンテンツをストレージ装置に蓄積する機能と、配信スケジュールに従って高速配信用ネットワーク３に出力する機能とを実現する装置である。ここでの出力機能は、広帯域伝送機能やレートコントロール機能を備える送信装置で実現される。

【０１５７】

高速配信用ネットワーク３を用いたデータの配信は現在のところ夜間を利用した蓄積型の配信を想定しているが、伝送速度の向上が期待される将来においてはストリーミング配信等も想定する。

【０１５８】

なお、ディジタルコンテンツの配信を記録媒体の形態で実行する場合、前述した出力機能はディジタルコンテンツを所定の記録媒体に格納する記録装置で実現される。

【０１５９】

コンテンツ管理サーバ１５は、コンテンツサーバ１１と通信し、新たに受付けたコンテンツの登録処理やコンテンツの検索処理、ファイル分割処理その他を実行する装置である。当該サーバもコンピュータ構成を採る。当該サーバではコンテンツ毎に発生された暗号鍵情報が管理される。例えば、コンテンツと対応する暗号鍵との関係がデータベースとして管理される。

【０１６０】

鍵発生部１６は、配信対象であるディジタルコンテンツ毎に固有の暗号鍵を生成する手段である。暗号鍵の発生に使用される暗号方式は運用時に広く採用されているものを使用する。すなわち、不正な解読が困難な最新の暗号化技術に従う。

【０１６１】

配信先管理サーバ１７は、コンテンツ毎に配信先と配信条件その他の業務データや配信先毎に生成した暗号鍵の情報をデータベースにより管理する装置である。ここでの配信条件には使用可能期間、出力可能回数その他の情報が含まれる。また当該サーバもコンピュータ構成を採る。

【０１６２】

図４に示すように、配信先管理サーバ１７は、コンテンツ制作者１のシステムにのみ設ける場合、電子配信事業者２のシステムにのみ設ける場合、両者のシステム内に設ける場合が考えられる。これは各配信先に固有の鍵情報を誰が配信するかはビジネス上の選択事項だからである。ただし、鍵情報を知り得る事業者は少ないほどシステム全体からみた秘匿性は高まるため、コンテンツ制作者１のシステム内に配置するのが望ましい。

【０１６３】

合わせ鍵生成部１８は、コンテンツ毎に生成された暗号鍵Ａを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ａ１及びＡ２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の合わせ鍵Ａ１及びＡ２が生成される。生成された合わせ鍵は、合わせ鍵生成部１８によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、合わせ鍵生成部１８は、合わせ鍵Ａ１をネットワークを介した配信用に不図示の通信

部に与え、残る合わせ鍵Ａ２を記録媒体を介した配信用に書込部１９に与える。

【０１６４】

書込部１９は、通知を受けた合わせ鍵Ａ２を所定の記録媒体に書き込むための装置である。書込部１９には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【０１６５】

次に、下流側システムを構成する各機能部を説明する。受信サーバ３１は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルコンテンツの受信機能と、配信を受けたディジタルコンテンツをストレージ装置に蓄積する機能と、再生スケジュールに従って復号サーバ３３に出力する機能とを実現する装置である。ここでの受信機能は、受信データに含まれる誤り訂正等を行う機能も備える。

【０１６６】

なお、ディジタルコンテンツの配信を記録媒体の形態で受ける場合、前述した受信機能はディジタルコンテンツを所定の記録媒体から読み取る読取装置で実現される。

【０１６７】

読取部３２は、記録媒体の形態で配信される合わせ鍵Ａ２を記録媒体から読み取るための装置である。ここで駆動機構には、記録媒体に応じたものが用いられる。また、図中では表していないが、広域ネットワークを介して配信を受ける合わせ鍵Ａ１の受信用に通信部が設けられている。

【０１６８】

復号サーバ３３は、ディジタルコンテンツに施されている暗号処理を解除する処理と、暗号が解除されたディジタルコンテンツに施されている符号化処理を復号化する処理とを実行する一方で、復元された生のディジタルコンテンツがそのまま装置外部に出力されないように局所的なスクランブル処理を施す装置である

。

【０１６９】

復号サーバ３３は、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。因みに当該復号サーバ３３は、悪意の特定者による不正行為からディジタルコンテンツを保護するため、正規の手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。これらの仕組みについては既存の技術を使用する。

【０１７０】

特に、復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）については、各機能ブロック間において重要な情報（暗号鍵や生のディジタルコンテンツ）が流れるため、不正行為を排除するための対策が重要であり、当該機能ブロック部分を半導体集積回路化したり、正規な手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【０１７１】

ここで、復号化部３５Ａは、鍵復元部３５Ｂから与えられる暗号鍵を用い、受信サーバ３１から読み出されたディジタルコンテンツに施されている暗号処理（条件付きアクセス処理）を解除する機能部である。当該機能は専用のハードウェアで実現することもできるし、ソフトウェア上の機能として実現することもできる。

【０１７２】

鍵復元部３５Ｂは、ネットワークを介して配信を受けた合わせ鍵Ａ１と記録媒体の形態で配信を受けた合わせ鍵Ａ２に基づいて、ディジタルコンテンツに施されている暗号処理を解除できる暗号鍵を復元する機能を実現する機能部である。復元された暗号鍵は鍵復元部３５Ｂの管理下において所定の期間保持される。当該確認には不揮発性メモリ、ハードディスクその他の記録媒体が用いられる。

【０１７３】

また鍵復元部３５Ｂは、受信サーバ３１から読み出されたディジタルコンテン

ツの暗号を復号するのに先だって、当該ディジタルコンテンツに付属されている業務データを読み出し、当該業務データで定められている再生条件が各時点において満たされているか否かの判定も行う。

【０１７４】

ここで、鍵復元部３５Ｂは、再生条件が満たされるとき、復号化部３５Ａに暗号解除許可信号を与える一方、スクランブル制御部３６にスクランブル鍵の発生信号又は出力許可信号を与える。これに対し、鍵復元部３５Ｂは、再生条件が満たされないとき、復号化部３５Ａに暗号解除禁止信号を与えると共に、スクランブル制御部３６にスクランブル鍵の発生禁止信号又は出力禁止信号を与える。

【０１７５】

コンテンツ復号化部３５Ｃは、特定者毎が採用しているコーデック方式に対応するものが用いられる。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。コンテンツ復号化部３５Ｃの信号処理の結果、暗号化処理前の生のディジタルコンテンツが復元される。

【０１７６】

スクランブル部３５Ｄは、コンテンツ復号化部３５Ｃによって復元されたディジタルコンテンツがそのままの形態で出力されることがないように、スクランブル処理を施すための装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１７７】

なお図４の場合、必要最小限の機能という意味でスクランブル制御部３６を復号機能部３５の外部においているが、スクランブル制御部３６を復号機能部３５内の一機能として設けることも可能である。

【０１７８】

スクランブル制御部３６は、鍵復元部３５Ｂによりスクランブル鍵の発生が許可された場合、スクランブル鍵とこれと対をなすデスクランブル鍵を発生する。

【０１７９】

なお、スクランブル鍵とデスクランブル鍵の発生方法には、コンテンツの違い

によらずいつも同じスクランブル鍵等を発生する方法（固定的に記憶されているスクランブル鍵とデスクランブル鍵を出力する方法）と、コンテンツ毎に異なるスクランブル鍵等を発生する方法（新たなコンテンツの出力のたび生成され、所定の再生条件が満たされる間保持される方法）と、再生出力のたびに異なるスクランブル鍵等を生成する方法（コンテンツの暗号を解除するたびに異なるスクランブル鍵を生成する方法）とがある。不正行為に対する防御機能の観点からは、記載順に３番目の方法、２番目の方法、１番目の方法の順番で不正が困難になる。

【０１８０】

出力ログ管理部３７は、出力装置３４からの不正出力を監視するため、出力装置３４における出力ログを管理する装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。出力ログ管理部３７は、出力ログを通信回線を通じて上流側システムを構成する配信先管理サーバ１７に通知する。この結果、上流側システムでも別途、各特定者の再生出力状況を監視できる。また不正行為の発見にも利用できる。

【０１８１】

最後に、出力装置３４の構成を説明する。出力装置３４は、ディジタルコンテンツに応じたものが用いられる。画像系であれば表示装置や投影装置が考えられるし、音声系であればスピーカが考えられる。いずれにしても、出力装置３４は、その本来の機能部の他にデスクランブル部３４Ａを備える。

【０１８２】

デスクランブル部３４Ａは、復号サーバ３３から与えられるディジタルコンテンツに施されているスクランブル処理を解除するための機能装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。当該デスクランブル部３４Ａは、半導体集積回路やボード部材で構成される。

【０１８３】

この出力装置３４の場合も、デスクランブル部３４Ａから出力される信号につ

いては、電子透かしのような静的な保護機能しか施されていないため、正規の手続き以外では出力装置の筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【０１８４】

（２－１－３）ディジタルコンテンツの配信動作

第１のシステムにおけるディジタルコンテンツの配信動作を簡単に説明する。当該システムでは、新たなディジタルコンテンツがコンテンツサーバ１１に登録されると、コンテンツ管理サーバ１５の管理下において当該コンテンツに固有の暗号鍵が発生される。次に、作成された暗号鍵が合わせ鍵生成部１８に与えられ、各配信者に固有の分割パターンによって固有の合わせ鍵が生成される。

【０１８５】

ここで、各配信者に固有の分割パターンはコンテンツの違いにかかわらず同じものでもよいし、コンテンツ毎に異なる分割パターンを採用してもよい。いずれにしても、特定者毎にコンテンツに固有の合わせ鍵が生成される。

【０１８６】

その後、生成された合わせ鍵Ａ１とＡ２がディジタルコンテンツの送信に先立って事前に配信される。このシステムの場合、合わせ鍵Ａ１はネットワークを通じて、合わせ鍵Ａ２は記録媒体に記録された形態で配信される。もっとも、常にディジタルコンテンツの配信に先立って行われなければならない訳ではない。暗号処理の解除に必要な鍵がディジタルコンテンツの配信後に行われる場合もあり得る。

【０１８７】

ディジタルコンテンツと合わせ鍵の配信を受けた下流側システムが、所定の出力スケジュールに従ってディジタルコンテンツを読み出し、復元された暗号鍵で暗号処理を解除する。その後、暗号処理の解除されたディジタルコンテンツのうち特定者のシステム構成に適合するコーデック方式にかかるものが選択的に復号化され、復号結果についてのスクランブル処理が復号サーバ３３にて実行される。

【０１８８】

この後、復号サーバ３３からはスクランブル処理が施されたディジタルコンテンツが出力装置３４に出力される。出力装置３４では、スクランブル制御部３６から与えられるデスクランブル鍵によってスクランブル処理の解除が行われ、所望の形態でコンテンツの出力が行われる。

【０１８９】

（２－１－４）第１のシステムによって得られる効果

上述のように第１のシステムによれば、合わせ鍵の配信経路を複数としたことにより、たとえいずれかの合わせ鍵が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、合わせ鍵をディジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、合わせ鍵の一部を盗んだ不正行為者が暗号化されたディジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルコンテンツとは別に配信されるため、生のディジタルコンテンツが復号化される事態を確実に回避できる。

【０１９０】

また、暗号処理が解除されたディジタルコンテンツにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。

【０１９１】

特に、運用後により安全性が高い暗号方式が出現した場合や取り扱うコーデック方式を変更したい場合でも、復号サーバ３３のみを置き換えることで対処できる。また、特定者が取り扱うコーデック方式が何であったとしても、復号サーバ３３から出力装置３４に出力されるデータはスクランブル処理されたデータに統一されるため、出力装置３４を複数のコーディク方式で共用できる。

【０１９２】

このことは出力装置３４の開発費が少なく済むことをも意味する。すなわち、汎用型の出力装置３４にデスクランブル部３４Ａを搭載すると共に、正規な手続きでしか開封できないか又は動作しない仕組みを搭載するだけでよいため、出力

装置３４の低価格化を実現できる。従って、運用後により性能の高い出力装置が開発された場合でも、例えば再現解像度の高いものが開発された場合でも、装置の置き換えが進み易い。

【０１９３】

かくして、不正行為に対する安全性もシステムを運用する上での経済性も同時に満足できる。

【０１９４】

（２－２）第２のシステム例

（２－２－１）システム構成

図５に、上述のビジネスモデルを実現するための第２のシステム例を示す。ここで図５は、図４との対応部分に同一符号を付して表したものである。図５と図４を対比して分かるように、当該システムを構成する下流側システムは第１のシステム例と同じである。

【０１９５】

本システムと第１のシステム例との違いは、合わせ鍵生成部１８で生成された合わせ鍵Ａ１を更に分割する部分鍵生成部２０が追加された点と、当該部分鍵生成部２０で生成された部分鍵を記録媒体に書き込むための書込部２１とその読み取り用の読取部３８が設けられた点と、配信される鍵情報が３つになったことに伴って鍵情報の配信方法に一部変更が生じた点である。

【０１９６】

部分鍵生成部２０は、合わせ鍵生成部１８の分割処理により得られた合わせ鍵の一部Ａ１を所定の分割パターンで分割し、一組の部分鍵Ａ１１及びＡ１２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の部分鍵Ａ１１及びＡ１２が生成される。なお所定の分割パターンは配信先毎に異なっていてもよいし、同じでもよい。

【０１９７】

生成された部分鍵は、部分鍵生成部２０によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、部分鍵生成部２０は、部分鍵Ａ１１をネットワークを介しての配信用に不図示の通信部に与え、残る部分鍵Ａ

１２を記録媒体による配信用に書込部２１に与える。

【０１９８】

書込部２１は、通知を受けた部分鍵Ａ１２を所定の記録媒体に書き込むための装置である。書込部２１には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【０１９９】

なお当該書込部２１と対をなす読取部３８には、配信を受ける記録媒体に応じた駆動機構を備えるものが用いられる。

【０２００】

また、第１のシステム例では、合わせ鍵生成部１８で生成された合わせ鍵Ａ２は記録媒体を通じて下流側システムに配信されていたが、この第２のシステム例の場合、合わせ鍵Ａ２はネットワークを介して配信される。

【０２０１】

以上が第２のシステム例と第１のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は部分鍵の発生以外同様に実行される。

【０２０２】

（２－２－２）第２のシステムによって得られる効果

以上のように第２のシステムによれば、鍵情報の配信を２つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するため、すなわち第１のシステムよりも更に鍵情報の配信経路が増えるため、伝送経路上での不正行為がより困難なものを提供できる。

【０２０３】

（２－３）第３のシステム例

（２－３－１）システム構成

図６に、上述のビジネスモデルを実現するための第３のシステム例を示す。ここで図６は、図４及び図５との対応部分に同一符号を付して表したものである。

【０２０４】

本システムにおける上流側システムと第２のシステム例との違いは、合わせ鍵Ａ２の配信がネットワークを介して行われるのではなく、第１のシステム例のように記録媒体を通じて実現される点である。このため、合わせ鍵Ａ２の配信経路については、第１のシステム例と同じものが用いられている。

【０２０５】

以上が第３のシステムと上述したシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第１のシステムや第２のシステムと同様である。

【０２０６】

（２－３－２）第３のシステムによって得られる効果

以上のように第３のシステムによれば、鍵情報の配信を１つの伝送網と２つの記録媒体とで実現するため、すなわち第２のシステムよりも記録媒体による配信経路が増えるため、鍵情報の盗難を発見し易いより不正行為に対する安全性の高いものを提供できる。

【０２０７】

（２－４）第４のシステム例

（２－４－１）システム構成

図７に、上述のビジネスモデルを実現するための第４のシステム例を示す。ここで図７は、図４との対応部分に同一符号を付して表したものである。

【０２０８】

本システムにおける上流側システムと第１のシステム例との違いは、合わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれもネットワークを介して配信される点である。

【０２０９】

以上が第４のシステムと第１のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は

第１のシステムと同様である。

【０２１０】

（２－４－２）第４のシステムによって得られる効果

以上のように第４のシステムによれば、鍵情報の配信を２つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【０２１１】

（２－５）第５のシステム例

（２－５－１）システム構成

図８に、上述のビジネスモデルを実現するための第５のシステム例を示す。ここで図８は、図４との対応部分に同一符号を付して表したものである。

【０２１２】

本システムにおける上流側システムと第１のシステム例との違いは、合わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれも記録媒体を介して配信される点である。このため、本システムでは、合わせ鍵Ａ１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２１３】

以上が第５のシステムと第１のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第１のシステムと同様である。

【０２１４】

（２－５－２）第５のシステムによって得られる効果

以上のように第５のシステムによれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２１５】

（２－６）第６のシステム例

（２－６－１）システム構成

図９に、上述のビジネスモデルを実現するための第６のシステム例を示す。ここで図９は、図５との対応部分に同一符号を付して表したものである。

【０２１６】

本システムにおける上流側システムと第２のシステム例（図５）との違いは、部分鍵生成部２０で発生された部分鍵Ａ１２がネットワークを介して配信される点である。

【０２１７】

以上が第６のシステムと第２のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第２のシステムと同様である。

【０２１８】

（２－６－２）第６のシステムによって得られる効果

以上のように第６のシステムによれば、鍵情報の配信を３つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【０２１９】

更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２２０】

（２－７）第７のシステム例

（２－７－１）システム構成

図１０に、上述のビジネスモデルを実現するための第７のシステム例を示す。ここで図１０は、図６及び図８との対応部分に同一符号を付して表したものであ

る。

【０２２１】

本システムにおける上流側システムと第３のシステム例との違いは、部分鍵生成部２０で発生された部分鍵Ａ１１及びＡ１２がいずれも記録媒体を介して配信される点である。このため、本システムでは、部分鍵Ａ１１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２２２】

以上が第７のシステムと第３のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第３のシステムと同様である。

【０２２３】

（２－７－２）第７のシステムによって得られる効果

以上のように第７のシステムによれば、鍵情報の配信を３つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２２４】

（２－８）第８のシステム例

（２－８－１）システム構成

図１１に、上述のビジネスモデルを実現するための第８のシステム例を示す。ここで図１１は、図４との対応部分に同一符号を付して表したものである。当該システムは、前述までの第１～第７のシステムとは異なり、ディジタルコンテンツの暗号鍵を分割するのではなく、当該暗号鍵を配信先に固有の別の多重鍵で暗号化する。

【０２２５】

このため、第８のシステムでは、配信先に固有の多重鍵Ｂを生成する多重鍵生成部２３と、当該多重鍵Ｂによって暗号鍵Ａを暗号化する鍵暗号化処理部２４と、多重鍵Ｂを記録媒体に書き込んで配信するのに使用する書込部２５と、これと

対をなす読取部４０を、第１のシステムにおける合わせ鍵生成部１８、書込部１９、読取部３２に置き換えて使用する。

【０２２６】

多重鍵生成部２３は、コンテンツ毎に生成された暗号鍵Ａに配信先毎に固有の暗号鍵Ｂを生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００通りの多重鍵Ｂを生成する。もっとも多重鍵Ｂは、配信先が同じであれば常に同じ多重鍵を用いる方法もあれば、コンテンツ毎に異なる多重鍵Ｂを生成して用いる場合もある。安全性の観点からは後者が望ましい。

【０２２７】

鍵暗号化処理部２４は、配信先毎に固有の多重鍵を用いて暗号鍵を暗号化する装置である。鍵暗号化処理部２４で暗号化された暗号鍵は、不図示の通信部よりネットワークを介して対応する下流側システムに配信される。

【０２２８】

書込部２５と読取部４０の構成は上述の書込部及び読取部と同じである。もっとも、書込部２５と読取部４０によって読み書きされるのは多重鍵である点で上述のシステムとは異なる。

【０２２９】

（２－８－２）ディジタルコンテンツの配信動作

第８のシステムにおけるディジタルコンテンツの配信動作のうち第１のシステムと異なる部分についてのみ簡単に説明する。すなわち、第１のシステムでは、コンテンツに固有の暗号鍵Ａを発生すると当該暗号鍵を合わせ鍵生成部１８に与えて合わせ鍵を生成したが、本システムの場合、配信先毎に発生された固有の多重鍵Ｂを用いて暗号鍵Ａを暗号化し、ネットワークを介して下流側システムに配信する。また、当該暗号鍵Ａの暗号化に使用した多重鍵Ｂをそれぞれ対応するは威信者に宛てて記録媒体の形態で配信する。

【０２３０】

なお生成された多重鍵Ｂは、配信先管理サーバ１７にて管理される。以上の処理動作が第１のシステムとの主な違いである。

【０２３１】

（２－８－３）第８のシステムによって得られる効果

上述のように第８のシステムによれば、下流側システムを管理する特定者に配信する鍵情報を暗号化された暗号鍵Ａと多重鍵Ｂとの２つとし、それらを複数の経路を介して配信する構成としたことにより、たとえいずれかの鍵情報が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。

【０２３２】

しかも多重鍵については盗難を発見し易い記録媒体の形態で配信を行うため、不正行為によって多重鍵が盗難されたことが明らかになった場合にはネットワークを介して行う暗号化された暗号鍵Ａの配信を行うのを中止し、別の多重鍵Ｂを記録媒体として配信する手順から再開することで不正行為に対する安全性を保つことができる。

【０２３３】

勿論、下流側システムの構成は第１のシステムと同じであるため、運用に際しての経済性にも優れることは第１のシステムと同様である。

【０２３４】

（２－９）第９のシステム例

（２－９－１）システム構成

図１２に、上述のビジネスモデルを実現するための第９のシステム例を示す。ここで図１２は、図１１との対応部分に同一符号を付して表したものである。

【０２３５】

本システムと第８のシステム例との違いは、多重鍵生成部２３で生成された多重鍵Ｂを分割し、一組の合わせ鍵Ｂ１とＢ２を生成する合わせ鍵生成部２６が追加された点と、当該合わせ鍵生成部２６で生成された合わせ鍵の一部Ｂ２を記録媒体に書き込むための書込部２７とその読み取り用の読取部４１が設けられた点である。

【０２３６】

合わせ鍵生成部２６は、配信先毎に生成された多重鍵Ｂを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ｂ１及びＢ２を生成する装置である。合わ

せ鍵生成部２６の分割規則は、全ての配信先について共通の分割規則を用いることも可能であるし、配信先毎に固有の分割規則を割り当てることも可能であるし、これら分割規則をコンテンツ単位で変更することも可能である。

【０２３７】

書込部２７と読取部４１の構成は他の書込部や読取部と同じである。なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第８のシステムと同様である。

【０２３８】

（２－９－２）第９のシステムによって得られる効果

以上のように第９のシステムによれば、多重鍵Ｂを一組の合わせ鍵Ｂ１及びＢ２に分割して一方をネットワークで、他方を記録媒体で配信する構成を採用するため、すなわち多重鍵Ｂそのものを送るのでなく分割したものを配信するのに加え、配信経路を２つから３つに増やすことにより、第８のシステムに比べてより不正行為に対する安全性の高いものを提供できる。

【０２３９】

（２－１０）第１０のシステム例

（２－１０－１）システム構成

図１３に、上述のビジネスモデルを実現するための第１０のシステム例を示す。ここで図１３は、図１２との対応部分に同一符号を付して表したものである。

【０２４０】

本システムと第９のシステム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。このため、本システムの場合には、書込部２８と読取部４２が新たに設けられる点で異なっている。書込部２８と読取部４２の構成は他の書込部や読取部と同じであるため省略する。

【０２４１】

なお基本的なシステム構成については何ら変更がないため、ディジタルコンテンツの配信動作は第８のシステムと同様である。

【０２４２】

（２－１０－２）第１０のシステムによって得られる効果

以上のように第１０のシステムによれば、暗号化された暗号鍵Ａが記録媒体を通じて配信される分、当該鍵がネットワークを介して配信される場合に比して盗難の早期発見が可能となり、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【０２４３】

（２－１１）第１１のシステム例

（２－１１－１）システム構成

図１４に、上述のビジネスモデルを実現するための第１１のシステム例を示す。ここで図１４は、図１１との対応部分に同一符号を付して表したものである。

【０２４４】

本システムと第８のシステムとの違いは、多重鍵Ｂを記録媒体を介して行うのではなく、ネットワークを介して行う点である。それ以外は第８のシステムと同じであるため、ディジタルコンテンツの配信動作は第８のシステムと同様である。もっとも、多重鍵Ｂの配信に際しては、ディジタル証明書等で相手方の正当性を確認した上で、配信先が公開している公開鍵で暗号化して配信するのが望ましい。

【０２４５】

（２－１１－２）第１１のシステムによって得られる効果

以上のように第１１のシステムによれば、多重鍵Ｂをネットワークを介して配信する手法を採用するため、鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【０２４６】

（２－１２）第１２のシステム例

（２－１２－１）システム構成

図１５に、上述のビジネスモデルを実現するための第１２のシステム例を示す。ここで図１５は、図１１及び図１３との対応部分に同一符号を付して表したものである。

【０２４７】

本システムと第８のシステム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。それ以外は第８のシステムと同じであるため、ディジタルコンテンツの配信動作は第８のシステムと同様である。

【０２４８】

（２－１２－２）第１２のシステムによって得られる効果

以上のように第１２のシステムによれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２４９】

（２－１３）第１３のシステム例

（２－１３－１）システム構成

図１６に、上述のビジネスモデルを実現するための第１３のシステム例を示す。ここで図１６は、図１２との対応部分に同一符号を付して表したものである。

【０２５０】

本システムと第９のシステムとの違いは、多重鍵Ｂから生成した合わせ鍵Ｂ２の配信に記録媒体を用いるのではなく、ネットワークを介して行う点である。すなわち、３つの鍵情報の配信を全てネットワークを介して行う点で異なっている。それ以外は第９のシステムと同じであるため、ディジタルコンテンツの配信動作は第９のシステムと同様である。

【０２５１】

（２－１３－２）第１３のシステムによって得られる効果

以上のように第１３のシステムによれば、鍵情報の配信を３つともネットワークを介して行うため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【０２５２】

更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワーク

を介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２５３】

（２－１４）第１４のシステム例

（２－１４－１）システム構成

図１７に、上述のビジネスモデルを実現するための第１４のシステム例を示す。ここで図１７は、図１３との対応部分に同一符号を付して表したものである。

【０２５４】

本システムと第１０のシステムとの違いは、多重鍵Ｂから生成した合わせ鍵Ｂ１の配信にネットワークを用いるのではなく、記録媒体を介して行う点である。すなわち、３つの鍵情報の配信を全て記録媒体を介して行う点で異なっている。このため、本システムの場合には、書込部２９と読取部４３が新たに設けられている。書込部２９と読取部４３の構成は他の書込部や読取部と同じであるため省略する。

【０２５５】

それ以外は第１０のシステムと同じであるため、ディジタルコンテンツの配信動作は第１０のシステムと同様である。

【０２５６】

（２－１４－２）第１４のシステムによって得られる効果

以上のように第１４のシステムによれば、鍵情報の配信を３つとも記録媒体を介して行うため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２５７】

（３）各システム例で想定される運用形態

第１～第１４のシステム例では、上流側システムを構成する機能部のいずれがコンテンツ制作会社１のシステム内で行われ、いずれが電子配信事業者２のシステム内で行われるか問題とすることなく、当該システム構成から認められる技術的な効果の観点から説明を行ったが、ここでは想定される運用形態についてビジ

ネス上の効果にどのような差異が生じるかについて説明する。特に、コンテンツ制作会社１の立場からみた得失について説明する。

【０２５８】

図１８は、上流側システムを構成する機能部のうち、コンテンツ符号化部１２と、暗号化部１３と、鍵発生部１６（間接的には合わせ鍵生成部（部分鍵生成部）や多重鍵生成部（その合わせ鍵生成部））がどのように配置されるかの観点からまとめたものである。ただし、図１８では、配信される鍵情報が２種類の場合について示されている。３種類以上の鍵情報が配信される場合には、図１８に「１つ」と表記された箇所は、「少なくとも１つ」を意味する。

【０２５９】

（３－１）第１の運用形態

第１の運用形態では、暗号鍵Ａの発生者、符号化処理の実行者、暗号処理の実行者のいずれもがコンテンツ制作会社である場合（すなわち、コンテンツ符号化部１２、暗号化部１３、鍵発生部１６がコンテンツ制作会社のシステム側に設けられる場合）であって、鍵情報の配信もコンテンツ制作会社が行う場合を考える。

【０２６０】

ここで、鍵情報の発生は配信主体であるコンテンツ制作会社が行う場合を想定する。すなわち、合わせ鍵生成部１８（システム例によっては部分鍵生成部２０も含む。）や多重鍵生成部２３及び鍵暗号化処理部２４（システム例によっては合わせ鍵生成部２６も含む。）もコンテンツ制作会社が行う場合を想定する。

【０２６１】

この場合、電子配信事業者２のシステムは暗号処理の施されたディジタルコンテンツを特定者に配信するだけの業務を行うことになる。すなわち、送出サーバ１４のみが電子配信事業者２のシステムに属することになる。

【０２６２】

このような運用形態を採ると、ディジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツ制作会社１のみとできる。このことは、コンテンツ制作会社１からみると、電子配信事業者２を通じて暗

号鍵が外部に流出する危険性を一切考慮しなくて済むため、安心してコンテンツの提供を行えるという利点がある。ただし、多くの信号処理を自前で行う必要があるため、設備投資を行う経済的余力のないコンテンツ作会社にとっては選択が難しい運用態様である。

【０２６３】

（３－２）第２の運用形態

第２の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体がコンテンツ制作会社１と電子配信事業者２の２者となる場合を考える。

【０２６４】

例えば、第２のシステム例（図５）において合わせ鍵Ａ２の生成と配信はコンテンツ制作会社１が行うが、合わせ鍵Ａ１から部分鍵Ａ１１とＡ１２を生成する処理と生成された部分鍵の配信は電子配信事業者２が行う場合が考えられる。この他同様の場合に、第３のシステム例（図６）、第６のシステム例（図９）、第７のシステム例（図１０）が考えられる。

【０２６５】

また例えば、生成された合わせ鍵や部分鍵の記録媒体への書込みと配信のみを電子配信事業者２に実行させる場合も考えられる。かかる場合には、第１のシステム例（図４）、第２のシステム例（図５）、第３のシステム例（図６において部分鍵Ａ１２及び又は合わせ鍵Ａ２を書き込む場合）、第５のシステム例（図８で合わせ鍵Ａ１又はＡ２を書き込む場合）、第７のシステム例（図１０でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）、第９のシステム例（図１２で合わせ鍵Ｂ２を書き込む場合）、第１０のシステム例（図１３で暗号化された暗号鍵又は合わせ鍵Ｂ２を書き込む場合）、第１２のシステム例（図１５で暗号化された暗号鍵を書き込む場合）、第１４のシステム例（図１７でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）がある。

【０２６６】

このような運用形態としても、ディジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツ制作者のみとなるため、コンテンツ制作会社１にとって安全な運用形態とできる。

【０２６７】

なお以上のものに比べるとやや信頼性は低下するが同様の効果が期待できるものに、第９のシステム例（図１２）において暗号鍵Ａの暗号化と配信はコンテンツ制作会社１が行うが、多重鍵Ｂの合わせ鍵Ｂ１、Ｂ２の生成と生成された合わせ鍵の配信は電子配信事業者２が行う場合が考えられる。

【０２６８】

これと同様のものに第１０のシステム例（図１３）、第１２のシステム例（図１５）、第１３のシステム例（図１６）、第１４のシステム例（図１７）が考えられる。

【０２６９】

（３－３）第３の運用形態

第３の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体が電子配信事業者２となる場合を考える。

【０２７０】

例えば、第１のシステム例（図４）において、暗号鍵の発生はコンテンツ制作会社１が行うが、発生された暗号鍵を入手して合わせ鍵Ａ１、Ａ２を生成する処理は電子配信事業者２が行う場合が考えられる。これはいずれのシステム例の場合にも考えられる。

【０２７１】

かかる運用形態を採ると、ディジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者がコンテンツ制作会社１と電子配信事業者２の２者となるため、第１の運用形態や第２の運用形態よりは暗号鍵が外部に流出する危険性が増えることになる。このため図１８では安全性を中程度としている。

【０２７２】

（３－４）第４～第６の運用形態

これらの運用形態では、第１～第３の運用形態と異なり、暗号化処理を電子配信事業者２が実行する場合を考える。すなわち、電子配信事業者２が暗号鍵をコンテンツ制作会社１から入手して暗号処理を実行する場合である。なお、これら

の例では符号化処理はコンテンツ制作会社１側が実行するものとする。

【０２７３】

これらの場合では、鍵情報の配信主体がコンテンツ制作会社１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社１と電子配信事業者２の２者となる。従って、コンテンツ制作会社の側からみた安全性は中程度となる。

【０２７４】

（３－５）第７～第９の運用形態

これらの運用形態では、第４～第６の運用形態に更に加えて、符号化処理の実行も電子配信事業者２が行う場合を考える。これらの運用形態では、コンテンツ制作会社１はもはや暗号鍵を生成しているだけにすぎず、鍵情報の配信主体がコンテンツ制作会社１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社１と電子配信事業者２の２者となる。従って、コンテンツ制作会社の側からみた安全性は中程度となる。

【０２７５】

（３－６）第１０～第１２の運用形態

これらの運用形態では、暗号鍵の生成を電子配信事業者２が行って、ディジタルコンテンツの暗号化は電子配信事業者２から暗号鍵の通知を受けたコンテンツ制作会社１が実施する場合を考える。この場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者はコンテンツ制作会社１と電子配信事業者２の２者となる。ただし、コンテンツ制作会社１は、暗号鍵の管理上は受身にならざる得ないので、コンテンツ制作会社の側からみた安全性は小さくなる。

【０２７６】

（３－７）第１３～第１８の運用形態

これらのうち第１３～第１５の運用形態は、暗号鍵の生成と暗号化処理を電子配信事業者２が実施し、符号化処理のみをコンテンツ事業者が行う場合である。また第１６～第１８の運用形態は、暗号鍵の生成、符号化処理、暗号化処理のい

ずれをも電子配信事業者２が行う場合である。

【０２７７】

いずれの運用形態の場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者はコンテンツ制作会社１と電子配信事業者２の２者となり、しかもコンテンツ制作会社１は、暗号鍵の管理上は受身にならざる得ないので、コンテンツ制作会社の側からみた安全性は小さくなる。

【０２７８】

【発明の効果】

（１）請求項１～１５のいずれかに記載の発明によれば、ディジタルコンテンツを各コンテンツに固有の暗号鍵で暗号化して配信する仕組みを採用することにより、あるディジタルコンテンツに対する被害が他のディジタルコンテンツに及ばない配信方法を実現できる。また、各コンテンツに固有の暗号鍵を基に生成される各特定者に固有の合わせ鍵や部分鍵を複数の配信経路を用いて個別に配信するようにしたことにより、暗号鍵を復元するのに必要な全ての情報を一度に入手するのが困難な配信方法を実現できる。また、下流側システムを、暗号処理の解除されたディジタルコンテンツにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な配信方法を実現できる。

【０２７９】

（２）請求項１６に記載の発明によれば、下流側システムを、暗号処理の解除されたディジタルコンテンツにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムを実現できる。

【０２８０】

（３）請求項１７に記載の発明によれば、その出力信号からはディジタルコンテンツの不正複製が困難な復号サーバを実現できる。また、請求項１８に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項１７の復号サーバと同様の機能を実現できる。また、請求項１９に記載の発明によれば、専用装置を用いなくても、請求項１７の復号サーバと同様の機能を実現することができ

る。また、請求項２０に記載の発明によれば、スクランブル制御部と別途組み合わせることで、請求項１７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項２１に記載の発明によれば、当該回路装置とスクランブル制御部とを別途組み合わせて電子機器に搭載するだけで請求項１７の復号サーバと同様の機能を実現できる。また、請求項２２に記載の発明によれば、コンピュータをスクランブル制御部として機能させるプログラムと組み合わせることで、専用装置を用いなくても、請求項１７の復号サーバと同様の機能を実現することができる。また、請求項２３に記載の発明によれば、請求項２０に記載の発明と組み合わせることで、請求項１７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項２４に記載の発明によれば当該回路装置と請求項２１に記載の回路装置とを別途組み合わせて電子機器に搭載するだけで請求項１７の復号サーバと同様の機能を実現できる。また、請求項２５に記載の発明によれば、請求項２２に記載のプログラムと組み合わせることで、専用装置を用いなくても、請求項１７の復号サーバと同様の機能を実現することができる。

【０２８１】

（４）請求項２６に記載の発明によれば、その入力信号からはディジタルコンテンツの不正複製が困難な出力装置を実現できる。また、請求項２７に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項２６の出力装置と同様の機能を実現できる。また、請求項２８に記載の発明によれば、専用装置を用いなくても、請求項２６の出力装置と同様の機能を実現することができる。

【０２８２】

（５）請求項２９に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルコンテンツにスクランブル処理を施して出力する仕組みを採用し、他方、出力装置がディジタルコンテンツに施されているスクランブル処理を解除して所定の出力形態で再生する仕組みを採用することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムにおける信号処理方法を実現できる。

【０２８３】

（６）請求項３０に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルコンテンツにスクランブル処理を施して出力する仕組みを採用することにより、その出力信号からはディジタルコンテンツの不正複製が困難な復号サーバにおける信号処理方法を実現できる。

【図面の簡単な説明】

【図１】

本発明にかかる配信システムの概念を説明する概念構成図である。

【図２】

本発明にかかる配信システムにおける高速配信用ネットワークで配信されるデータのデータ構造を示す図である。

【図３】

本発明にかかる配信システムを映画コンテンツに適用した場合について示す図である。

【図４】

本発明の実施の形態における第１の配信システムの構成例を示すブロック図である。

【図５】

本発明の実施の形態における第２の配信システムの構成例を示すブロック図である。

【図６】

本発明の実施の形態における第３の配信システムの構成例を示すブロック図である。

【図７】

本発明の実施の形態における第４の配信システムの構成例を示すブロック図である。

【図８】

本発明の実施の形態における第５の配信システムの構成例を示すブロック図である。

【図９】

本発明の実施の形態における第６の配信システムの構成例を示すブロック図である。

【図１０】

本発明の実施の形態における第７の配信システムの構成例を示すブロック図である。

【図１１】

本発明の実施の形態における第８の配信システムの構成例を示すブロック図である。

【図１２】

本発明の実施の形態における第９の配信システムの構成例を示すブロック図である。

【図１３】

本発明の実施の形態における第１０の配信システムの構成例を示すブロック図である。

【図１４】

本発明の実施の形態における第１１の配信システムの構成例を示すブロック図である。

【図１５】

本発明の実施の形態における第１２の配信システムの構成例を示すブロック図である。

【図１６】

本発明の実施の形態における第１３の配信システムの構成例を示すブロック図である。

【図１７】

本発明の実施の形態における第１４の配信システムの構成例を示すブロック図である。

【図１８】

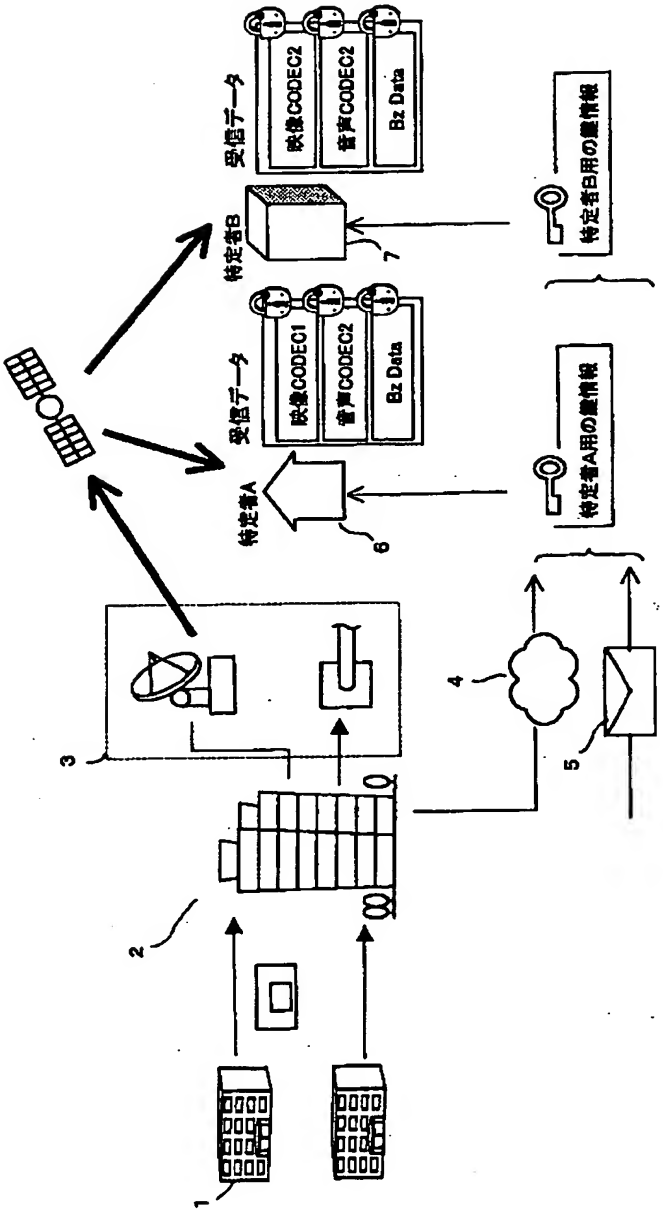
本発明の実施の形態の構成例として示す各配信システムに共通する運用形態を表示した図である。

【符号の説明】

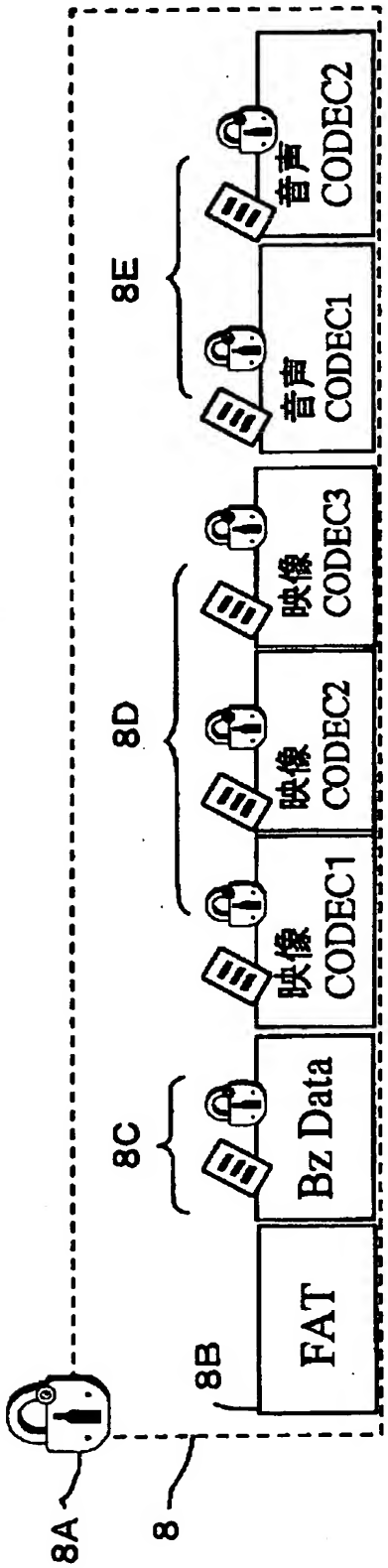
１　コンテンツサーバ、１２　コンテンツ符号化部、１３　暗号化部、１４　送出サーバ、１５　コンテンツ管理サーバ、１６　鍵発生部、１７　配信先管理サーバ、１８，２６　合わせ鍵生成部、１９，２１，２２，２５，２７，２８，２９　書込部、２０　部分鍵生成部、２３　多重鍵生成部、２４　鍵暗号化処理部、３１　受信サーバ、３２，３８，３９，４０，４１，４２，４３　読取部、３３　復号サーバ、３４　出力装置、３４Ａ　デスクランブル部、３５　復号機能部、３５Ａ　復号化部、３５Ｂ　鍵復元部、３５Ｃ　コンテンツ復号化部、３５Ｄ　スクランブル部、３６　スクランブル制御部、３７　出力ログ管理部

【書類名】　　図面

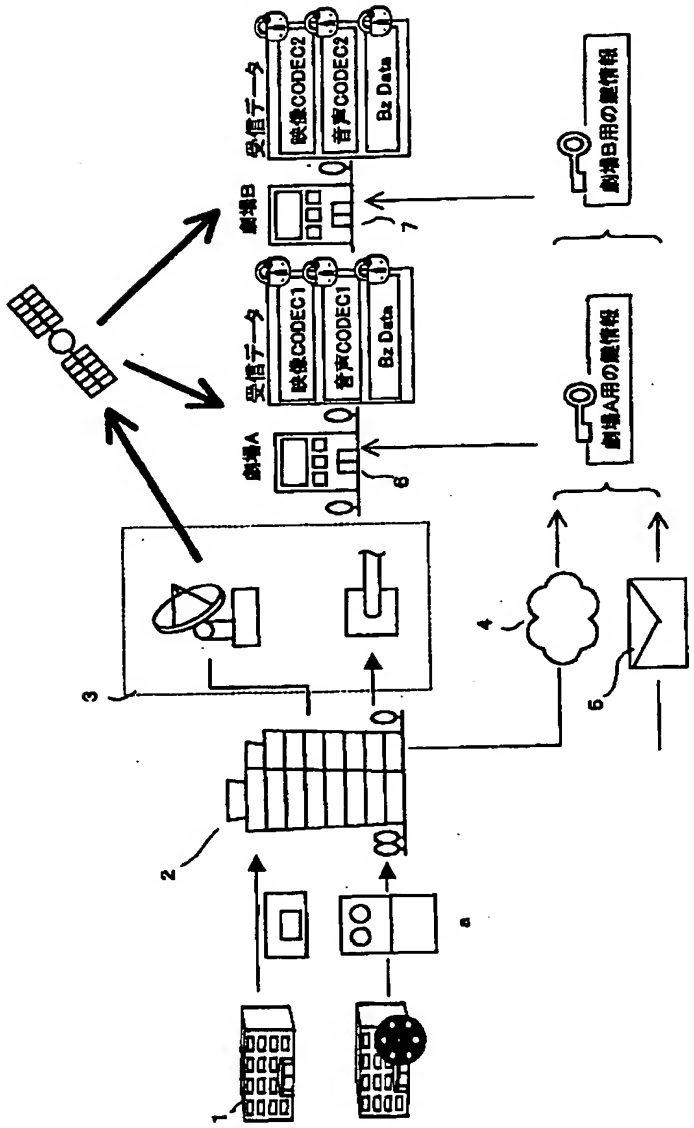
【図１】


受信データ
映像CODEC2
音声CODEC2
Bz Data
特定者B
7
特定者B用の鍵情報
受信データ
映像CODEC1
音声CODEC2
Bz Data
特定者A
6
特定者A用の鍵情報
3
4
5
2
1

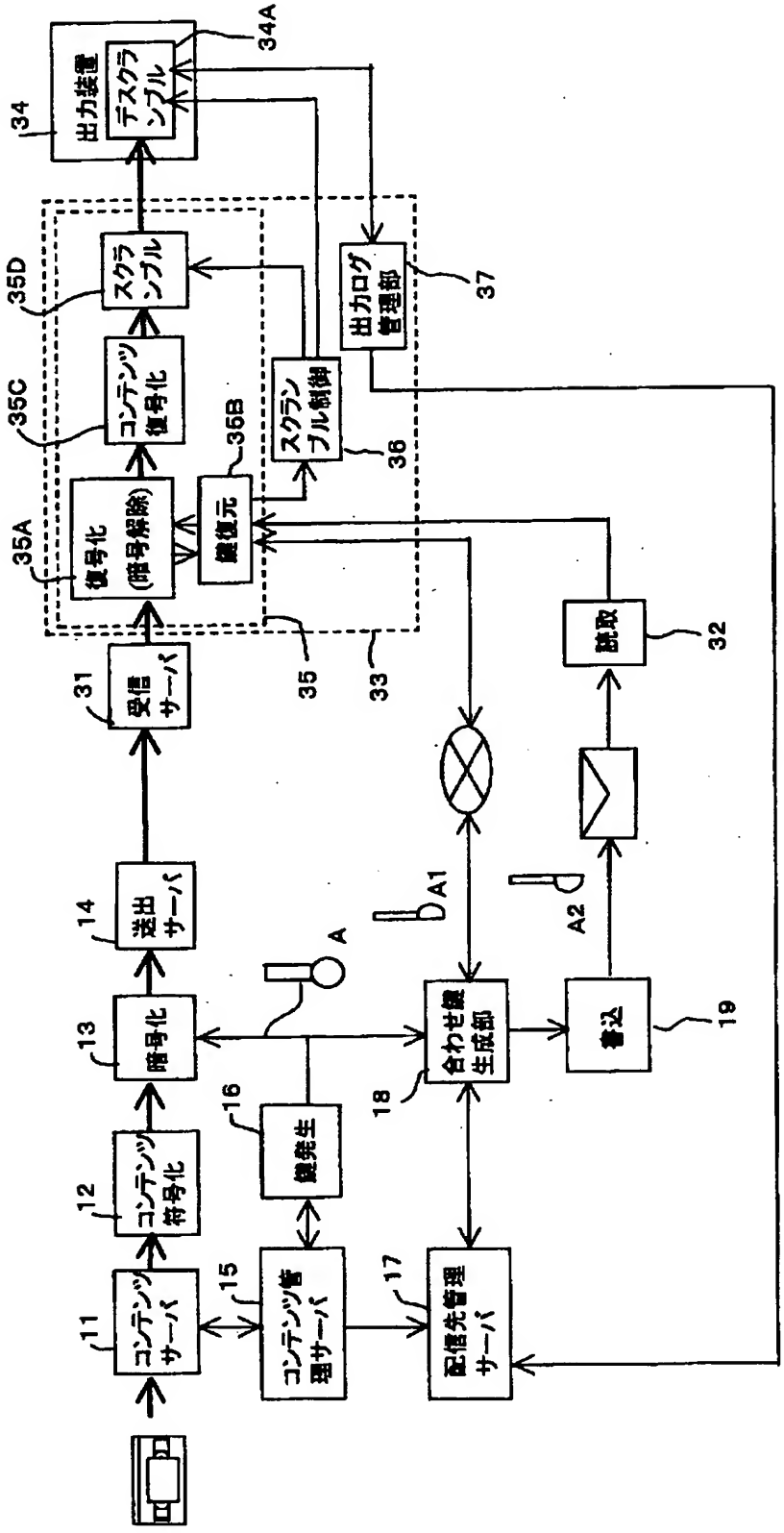
【図２】


8A
8
8B
FAT
8C
Bz Data
8D
映像 CODEC1
映像 CODEC2
映像 CODEC3
8E
音声 CODEC1
音声 CODEC2

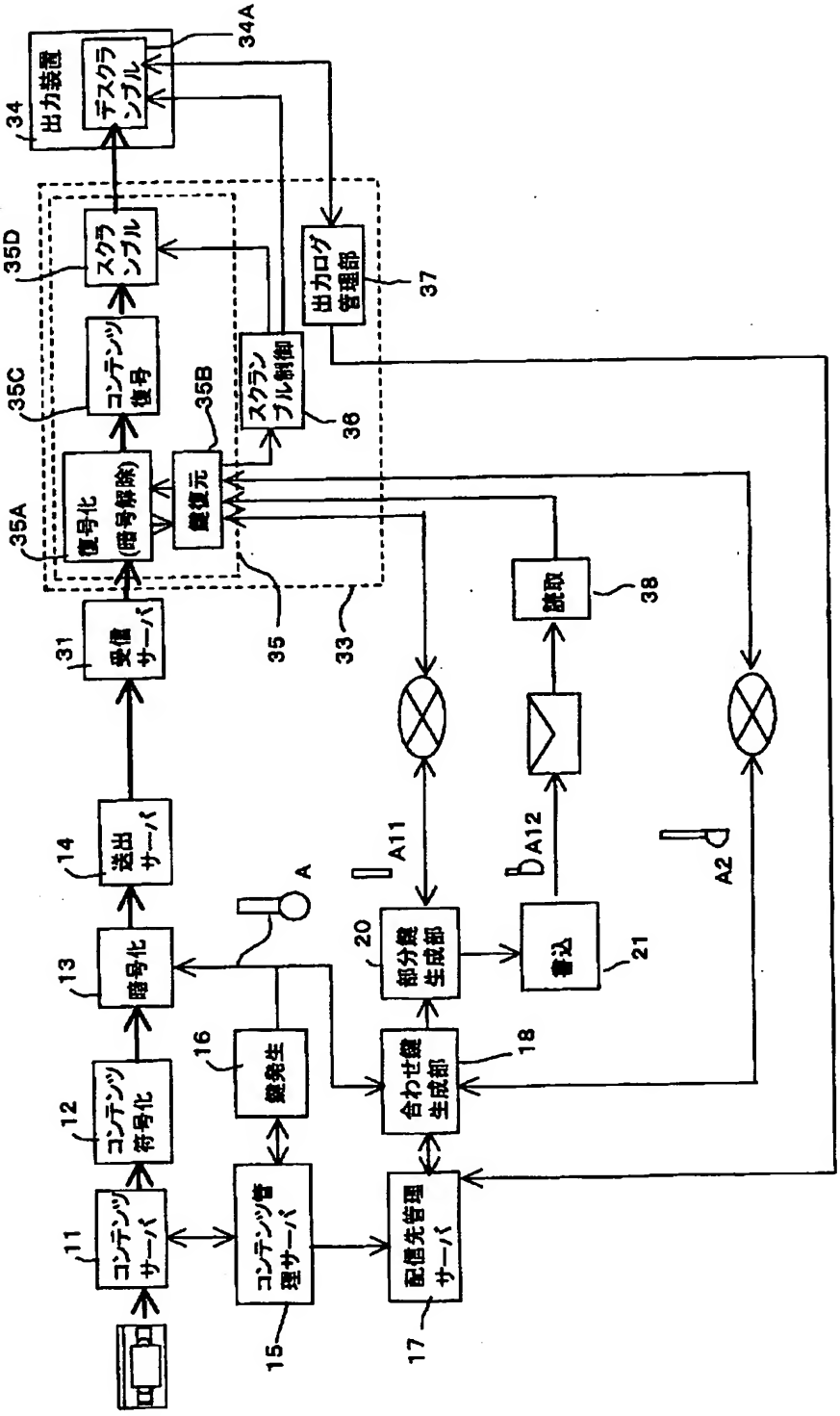
【図３】


受信データ
映像CODEC2
音声CODEC2
Bz Data
劇場B
劇場B用の鍵情報
受信データ
映像CODEC1
音声CODEC1
Bz Data
劇場A
劇場A用の鍵情報
1
2
3
4
5
6
7
8

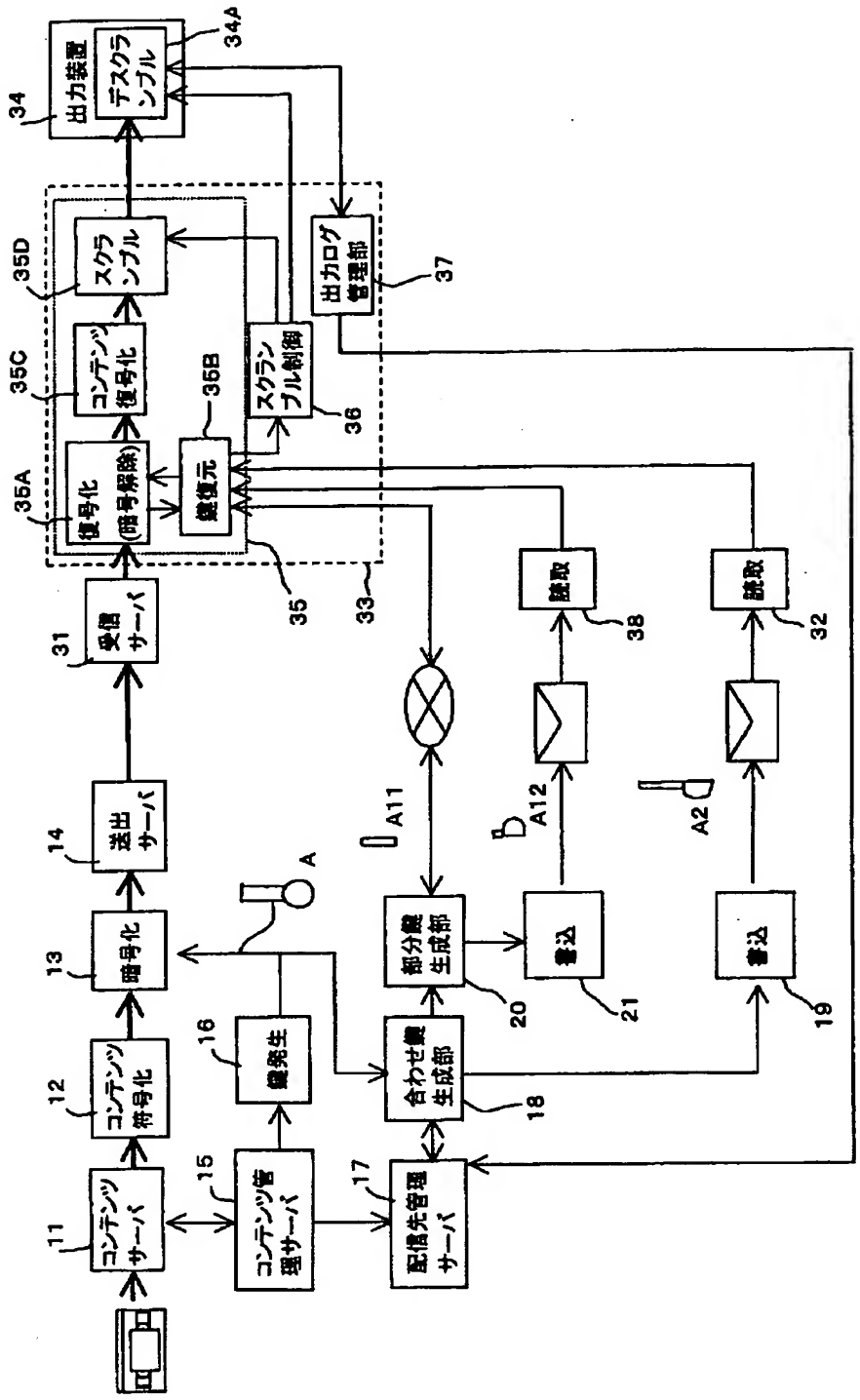
【図４】


出力装置
デスクラ
シブル
34
34A
スクラ
シブル
35D
コンテンツ
復号化
35C
復号化
(暗号解除)
35A
鍵復元
36B
スクラン
ブル制御
36
出力ログ
管理部
37
受信
サーバ
31
35
33
鍵取
32
送出
サーバ
14
暗号化
13
A
A1
A2
合わせ鍵
生成部
18
書込
19
鍵発生
16
コンテンツ
符号化
12
コンテンツ
サーバ
11
コンテンツ管
理サーバ
15
配信先管理
サーバ
17

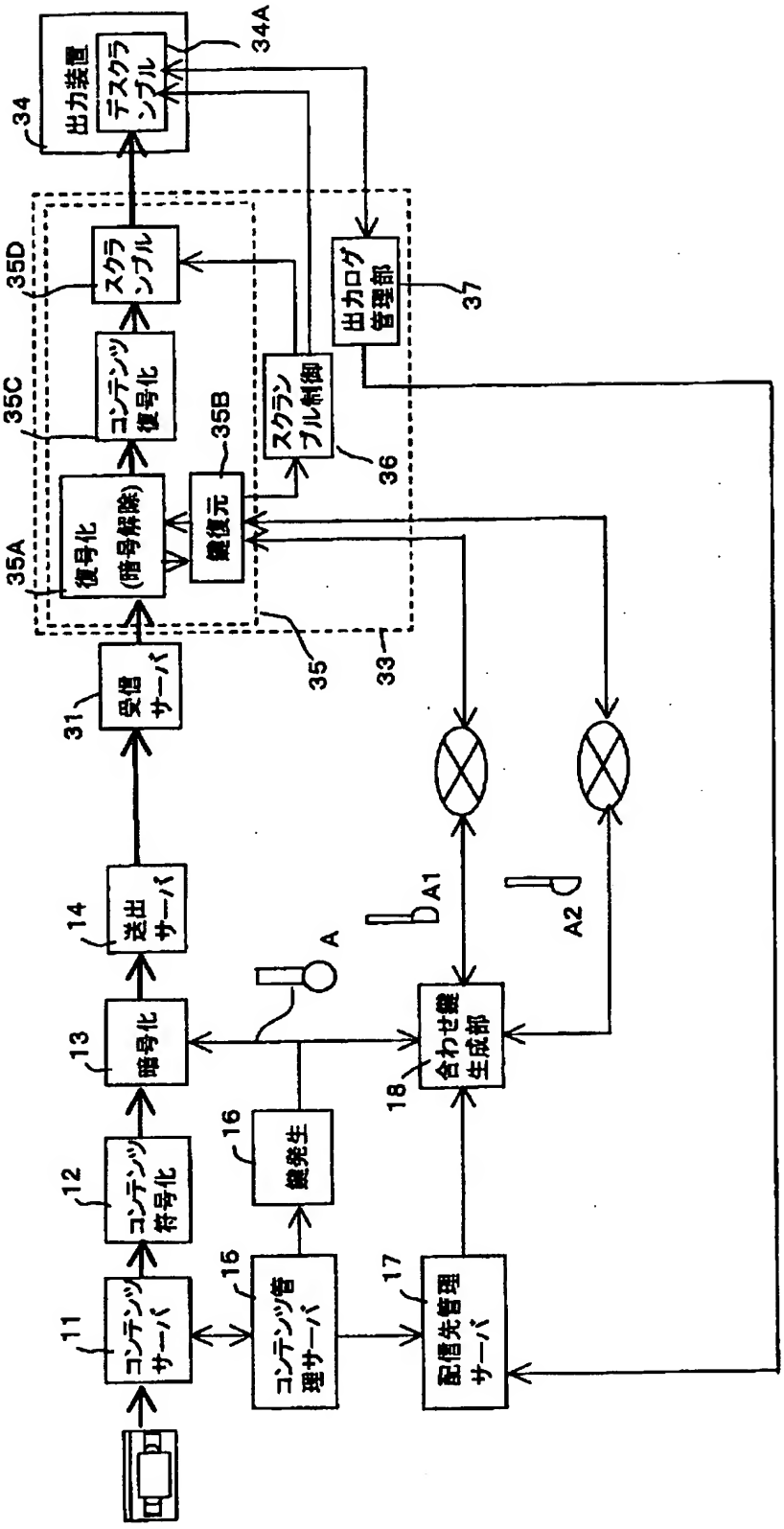
【図５】


34
出力装置
デスクランブル
34A
35D
スクランブル
出力ログ管理部
37
35C
コンテンツ復号
35B
スクランブル制御
36
35A
復号化(暗号解除)
鍵復元
31
受信サーバ
35
33
課取
38
14
送出サーバ
A11
A12
A2
A
13
暗号化
20
部分鍵生成部
書込
21
12
コンテンツ符号化
16
鍵発生
合わせ鍵生成部
18
11
コンテンツサーバ
コンテンツ管理サーバ
配信先管理サーバ
15
17

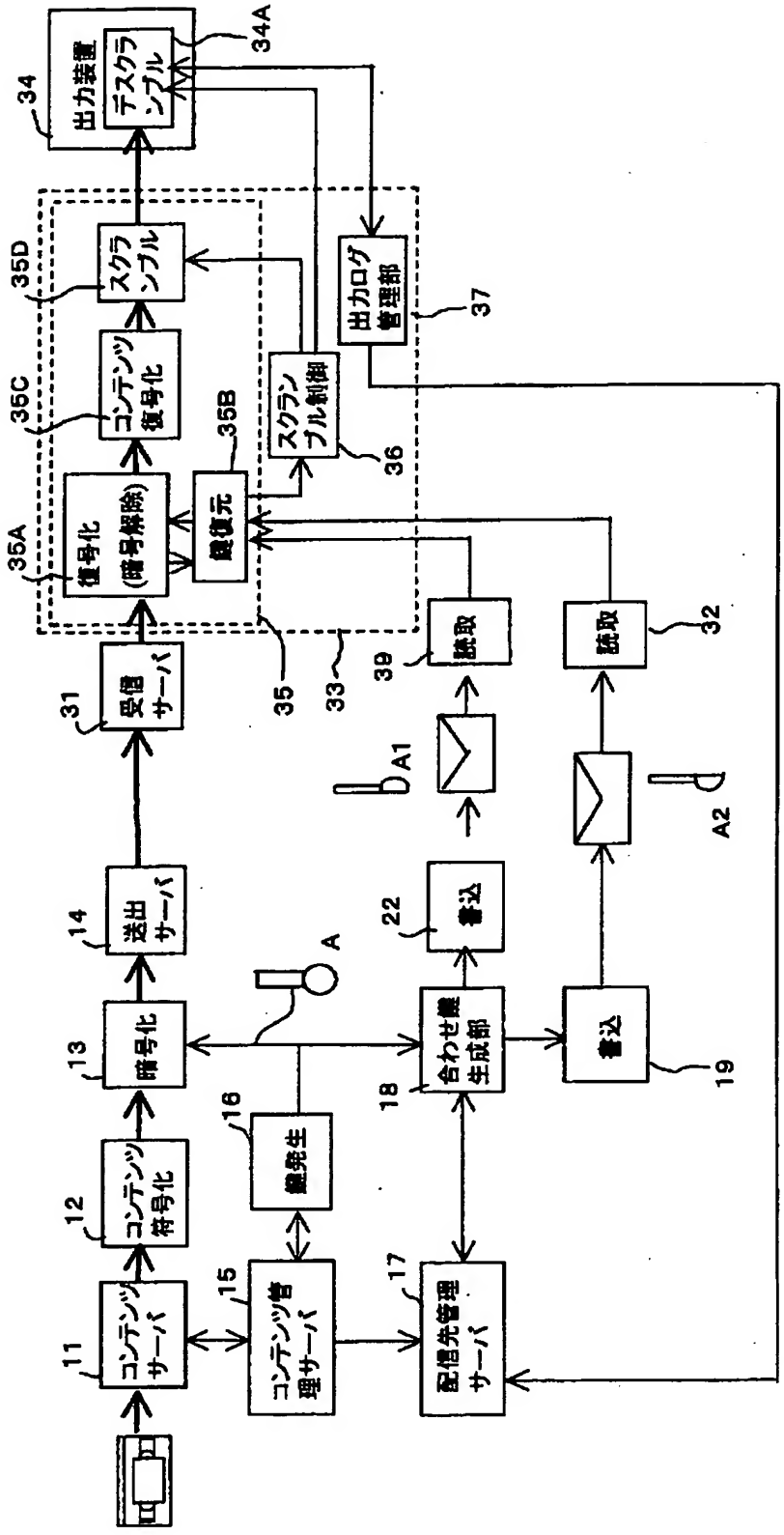
【図６】


出力装置
34
デスクランブル
34A
スクランブル
35D
コンテンツ復号化
35C
復号化（暗号解除）
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
コンテンツ管理サーバ
15
鍵発生
16
配信先管理サーバ
17
合わせ鍵生成部
18
部分鍵生成部
20
書込
21
書込
19
A
A11
A12
A2
B
抜取
38
抜取
32

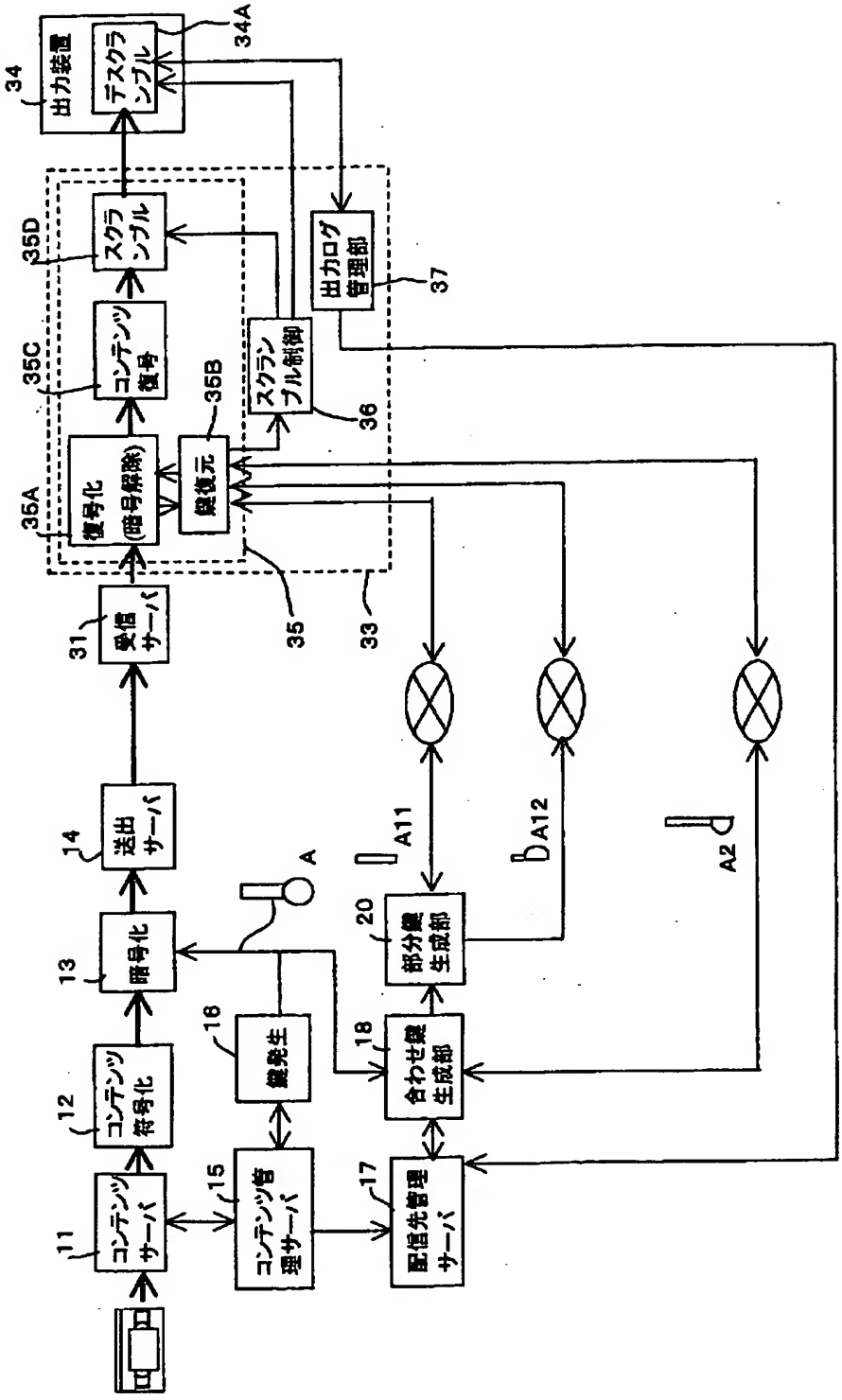
【図７】


出力装置
34
デスクラシンプル
34A
スクラシンプル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
16
合わせ鍵生成部
18
配信先管理サーバ
17
A
A1
A2

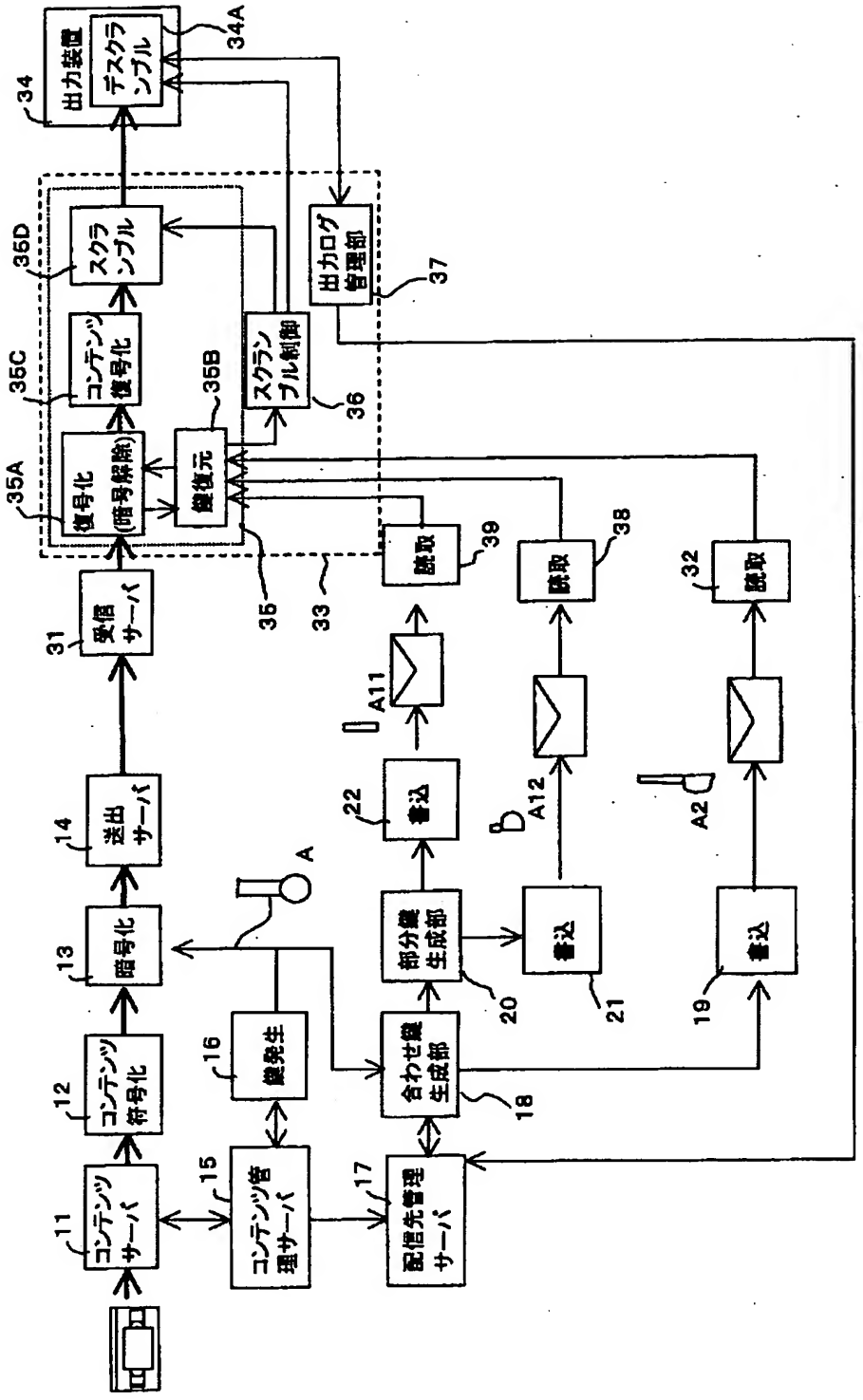
【図８】


出力装置
34
デスクランブル
34A
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
15
配信先管理サーバ
17
合わせ鍵生成部
18
書込
22
書込
19
読取
39
読取
32
35
33
A
A1
A2

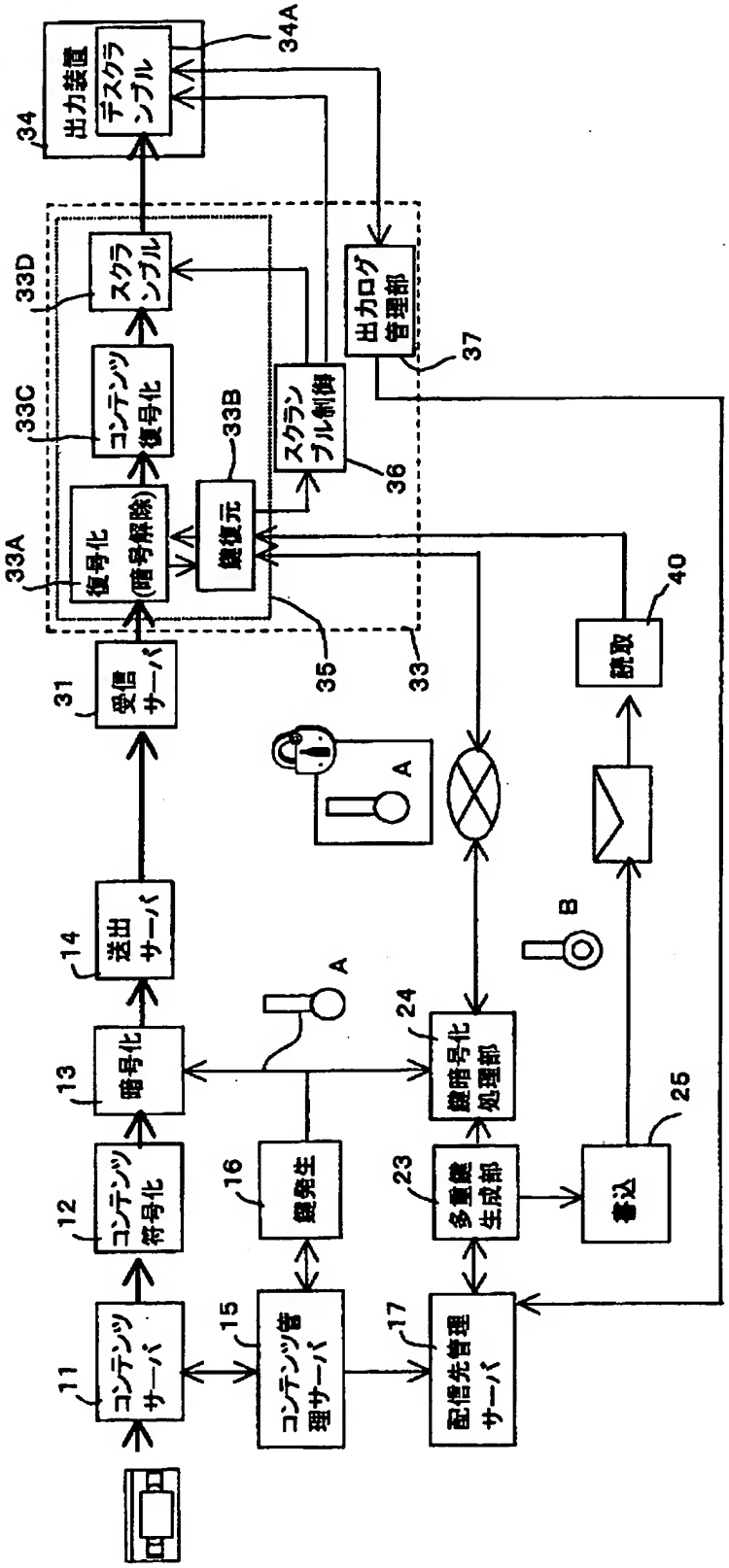
【図９】


34
出力装置
34A
デスクラシンプル
35D
スクラシンプル
出力ログ管理部
37
35C
コンテンツ復号
35B
スクランブル制御
36
36A
復号化(暗号解除)
鍵復元
35
33
31
受信サーバ
14
送出サーバ
A
A11
A12
A2
20
部分鍵生成部
13
暗号化
16
鍵発生
18
合わせ鍵生成部
12
コンテンツ符号化
15
コンテンツ管理サーバ
17
配信先管理サーバ
11
コンテンツサーバ

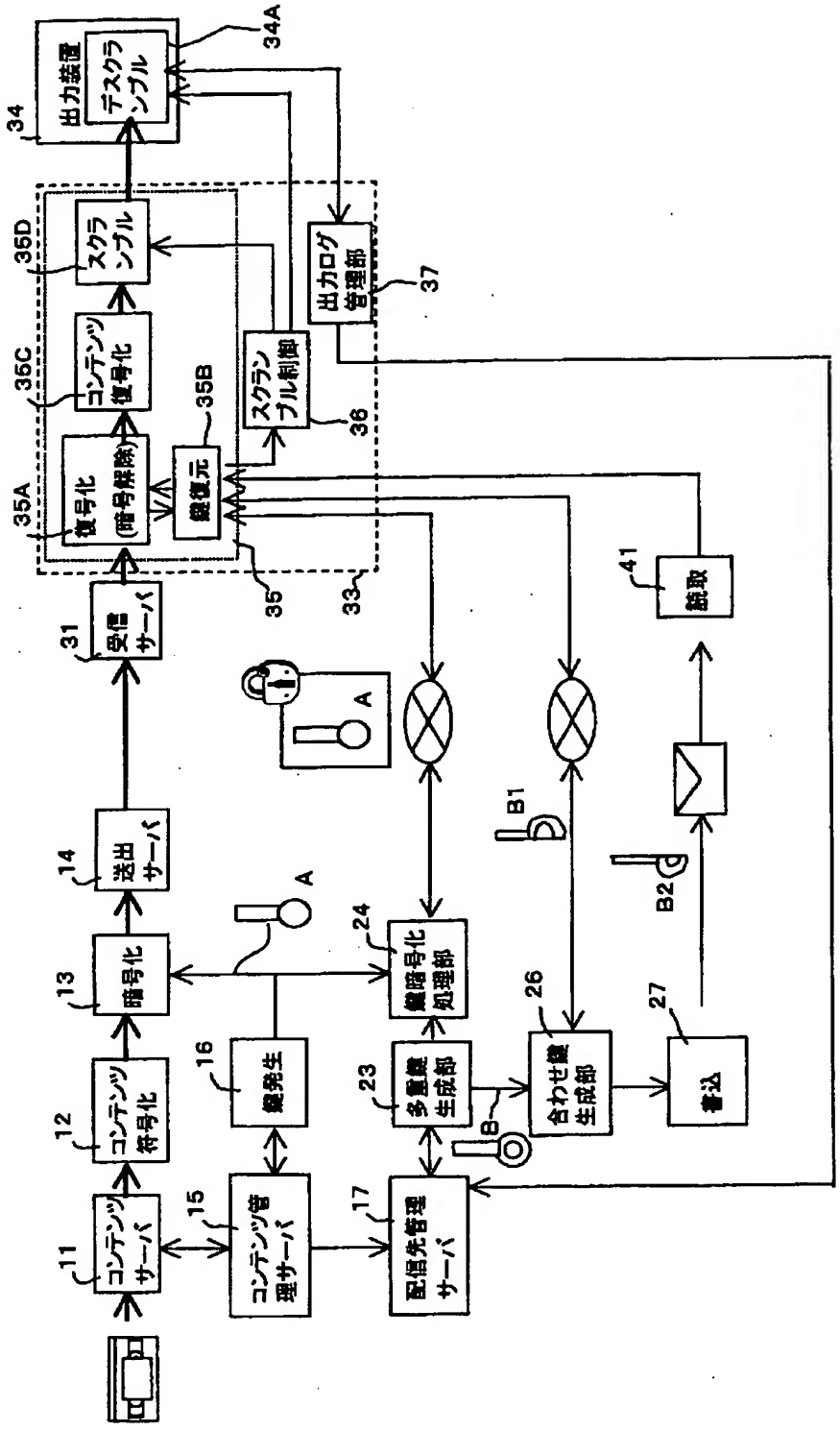
【図１０】


出力装置
34
デスクランブル
34A
スクランブル
35D
出力ログ管理部
37
コンテンツ暗号化
35C
スクランブル制御
35B
36
復号化（暗号解除）
35A
鍵復元
35
33
鍵取
39
鍵取
38
鍵取
32
受信サーバ
31
A11
送出サーバ
14
書込
22
A12
A2
暗号化
13
A
部分鍵生成部
書込
書込
20
21
19
コンテンツ符号化
12
鍵発生
16
合わせ鍵生成部
18
コンテンツサーバ
11
コンテンツ管理サーバ
15
配信先管理サーバ
17

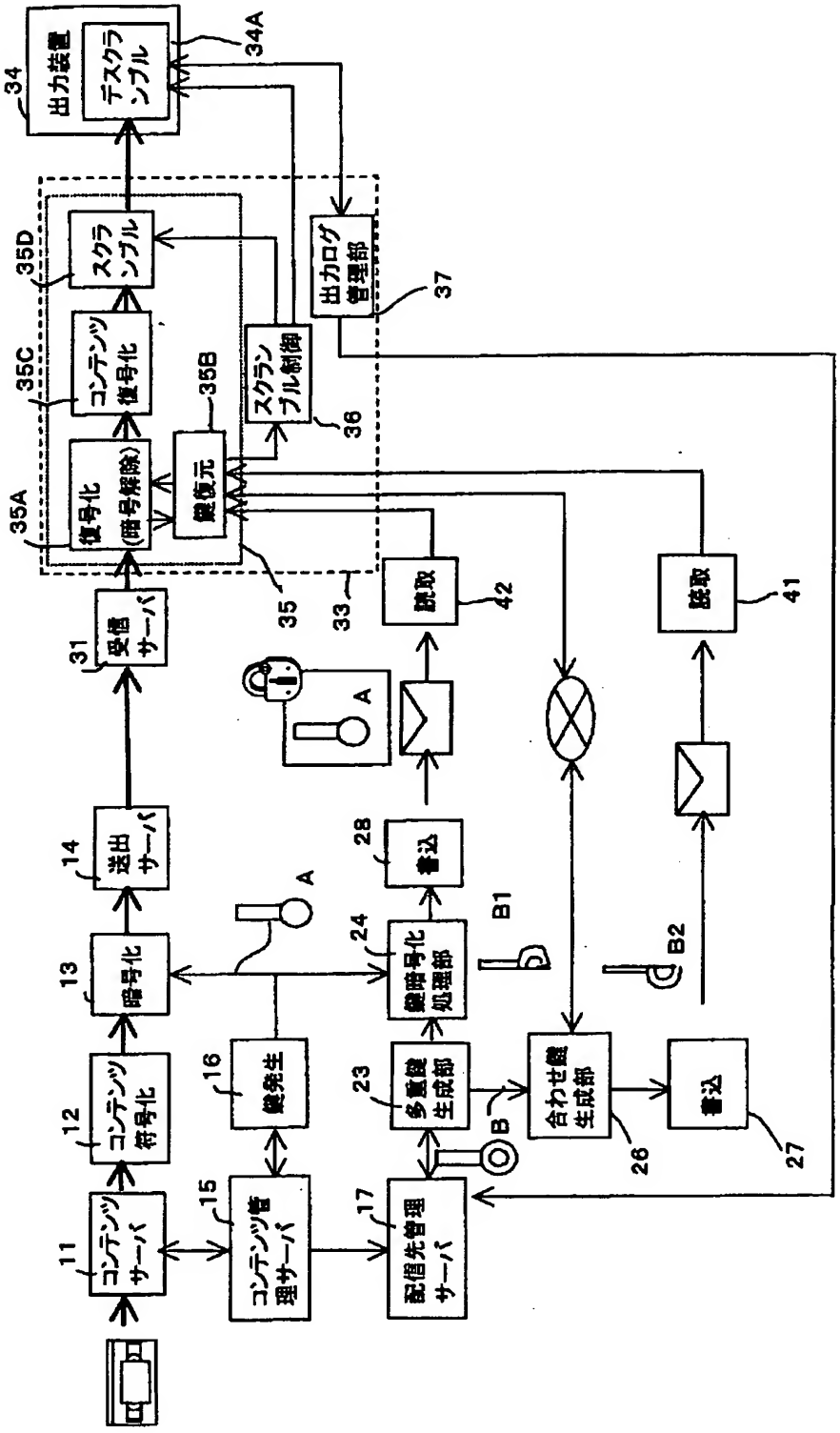
【図１１】


34
出力装置
デスクランブル
34A
33D
スクランブル
33C
コンテンツ復号化
33B
スクランブル制御
出力ログ管理部
37
36
33A
復号化（暗号解除）
鍵復元
40
取得
31
受信サーバ
35
33
A
14
送出サーバ
B
A
24
鍵暗号化処理部
13
暗号化
25
12
コンテンツ符号化
16
鍵発生
23
多重鍵生成部
書込
11
コンテンツサーバ
15
コンテンツ管理サーバ
17
配信先管理サーバ

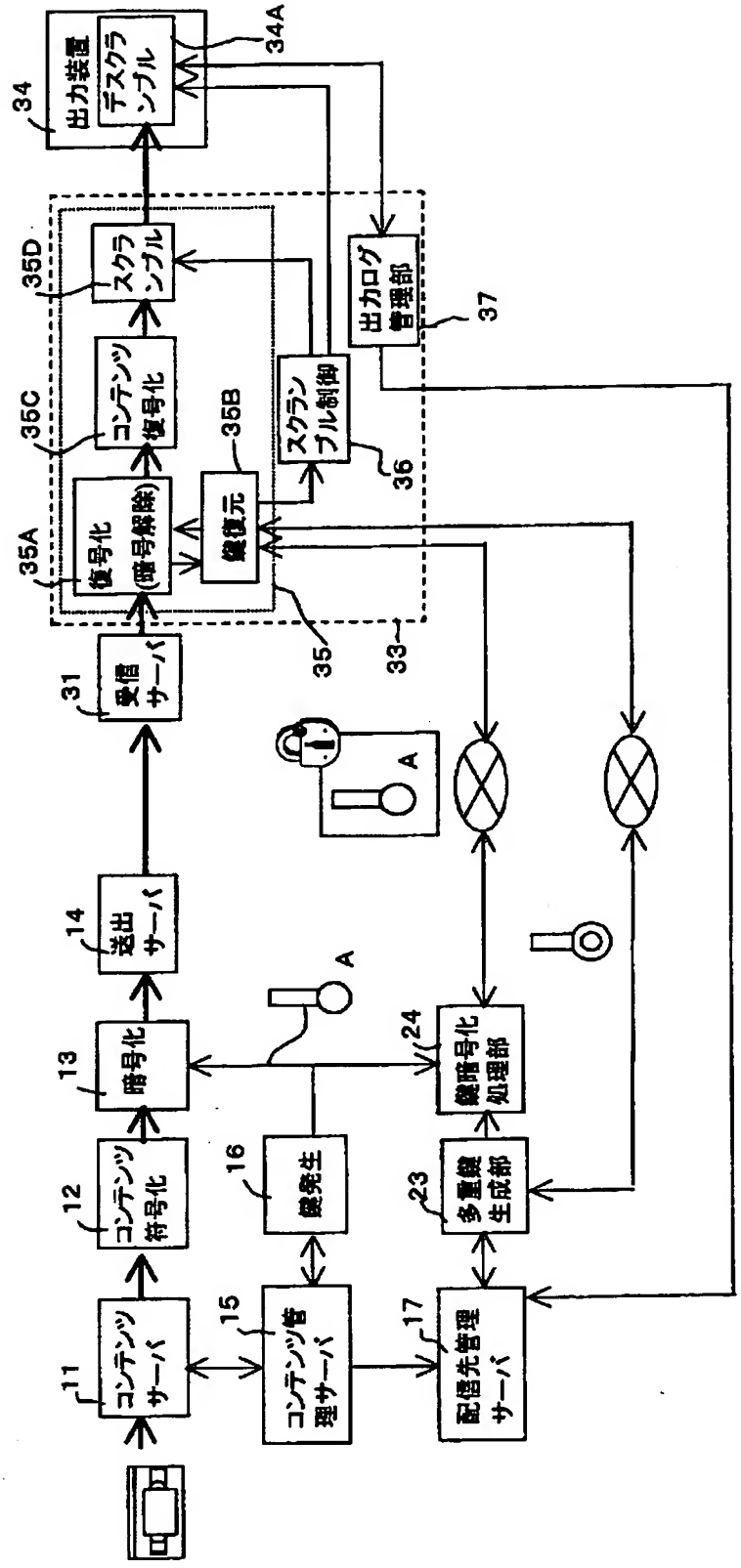
【図１２】


出力装置
デスクラ
シンプル
34
34A
スクラ
シンプル
35D
コンテンツ
復号化
35C
復号化
(暗号解除)
35A
鍵復元
35B
スクラン
ブル制御
36
出力ログ
管理部
37
35
33
受信
サーバ
31
送出
サーバ
14
暗号化
13
コンテンツ
符号化
12
コンテンツ
サーバ
11
鍵発生
16
コンテンツ管
理サーバ
15
鍵暗号化
処理部
24
多重鍵
生成部
23
配信先管理
サーバ
17
合わせ鍵
生成部
26
書込
27
鍵取
41
A
A
B1
B2
B

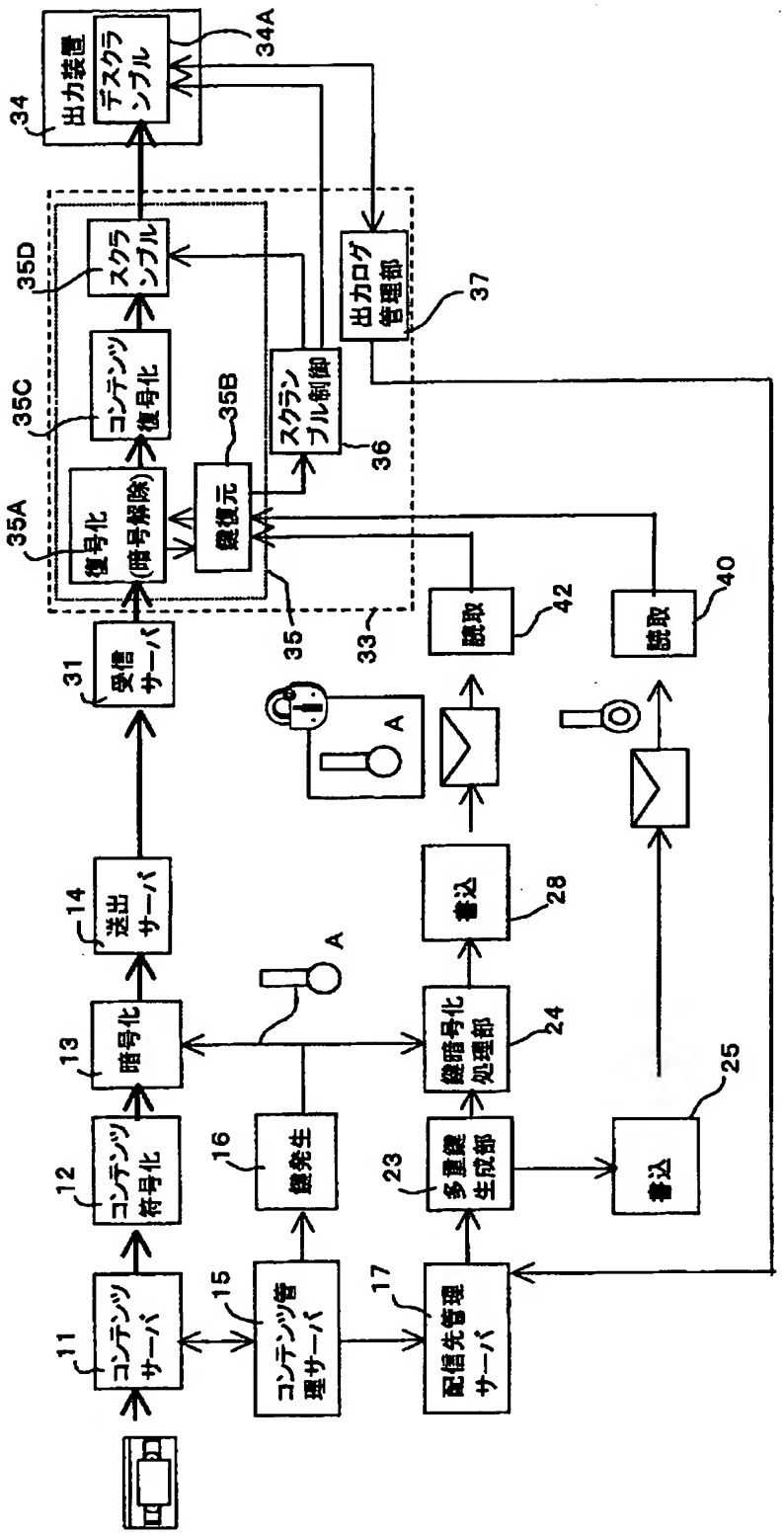
【図１３】


34
出力装置
34A
デスクランブル
35D
スクランブル
出力ログ管理部
37
35C
コンテンツ復号化
35B
スクランブル制御
36
35A
復号化(暗号解除)
鍵復元
35
33
31
受信サーバ
A
読取
42
読取
41
14
送出サーバ
28
書込
A
B1
B2
24
鍵暗号化処理部
13
暗号化
16
鍵発生
23
多重鍵生成部
合わせ鍵生成部
書込
27
26
12
コンテンツ符号化
B
11
コンテンツサーバ
15
コンテンツ管理サーバ
17
配信先管理サーバ

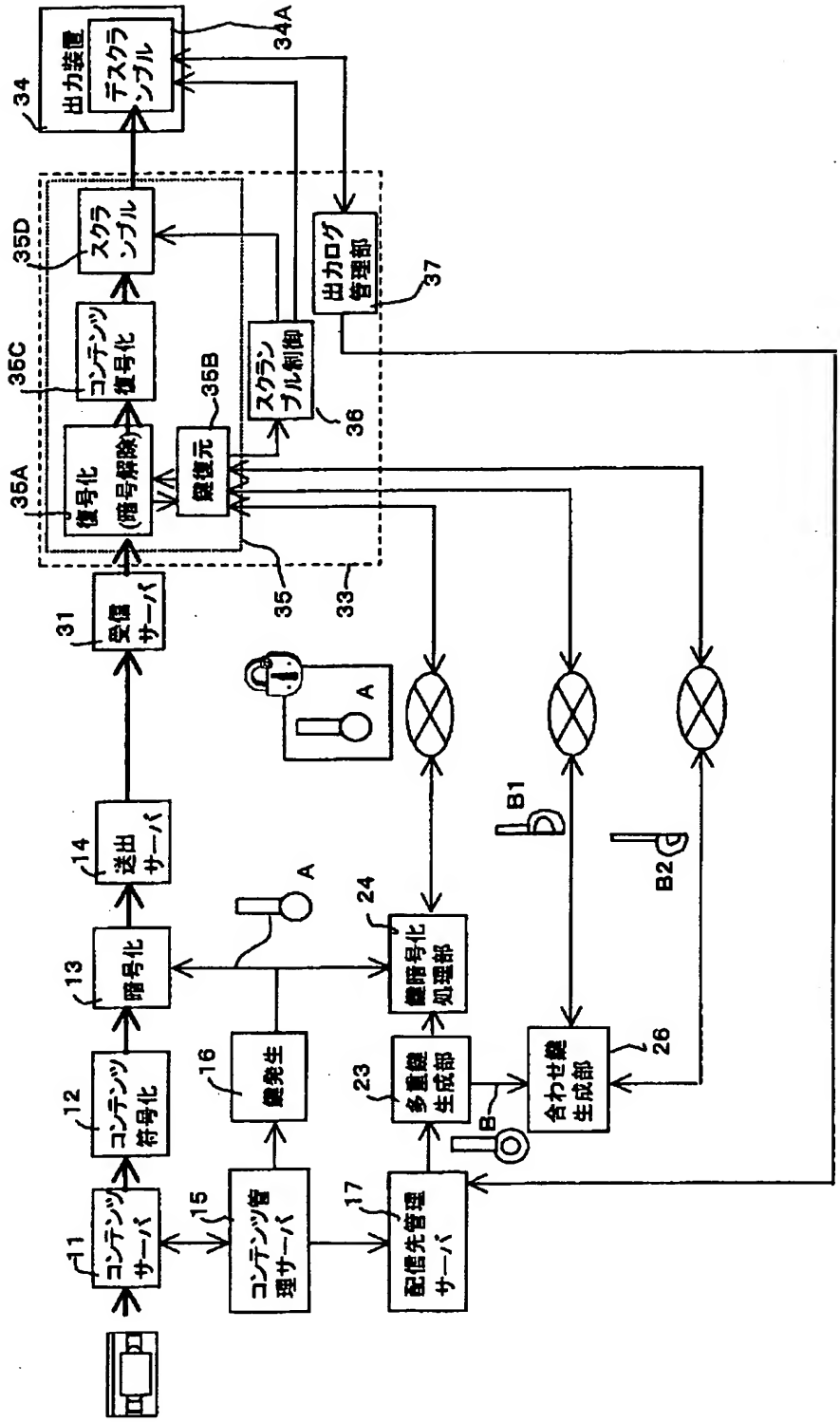
【図１４】


出力装置
デスクランブル
34A
34
出力ログ管理部
37
スクランブル制御
36
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
15
鍵暗号化処理部
24
多重鍵生成部
23
配信先管理サーバ
17
A
A

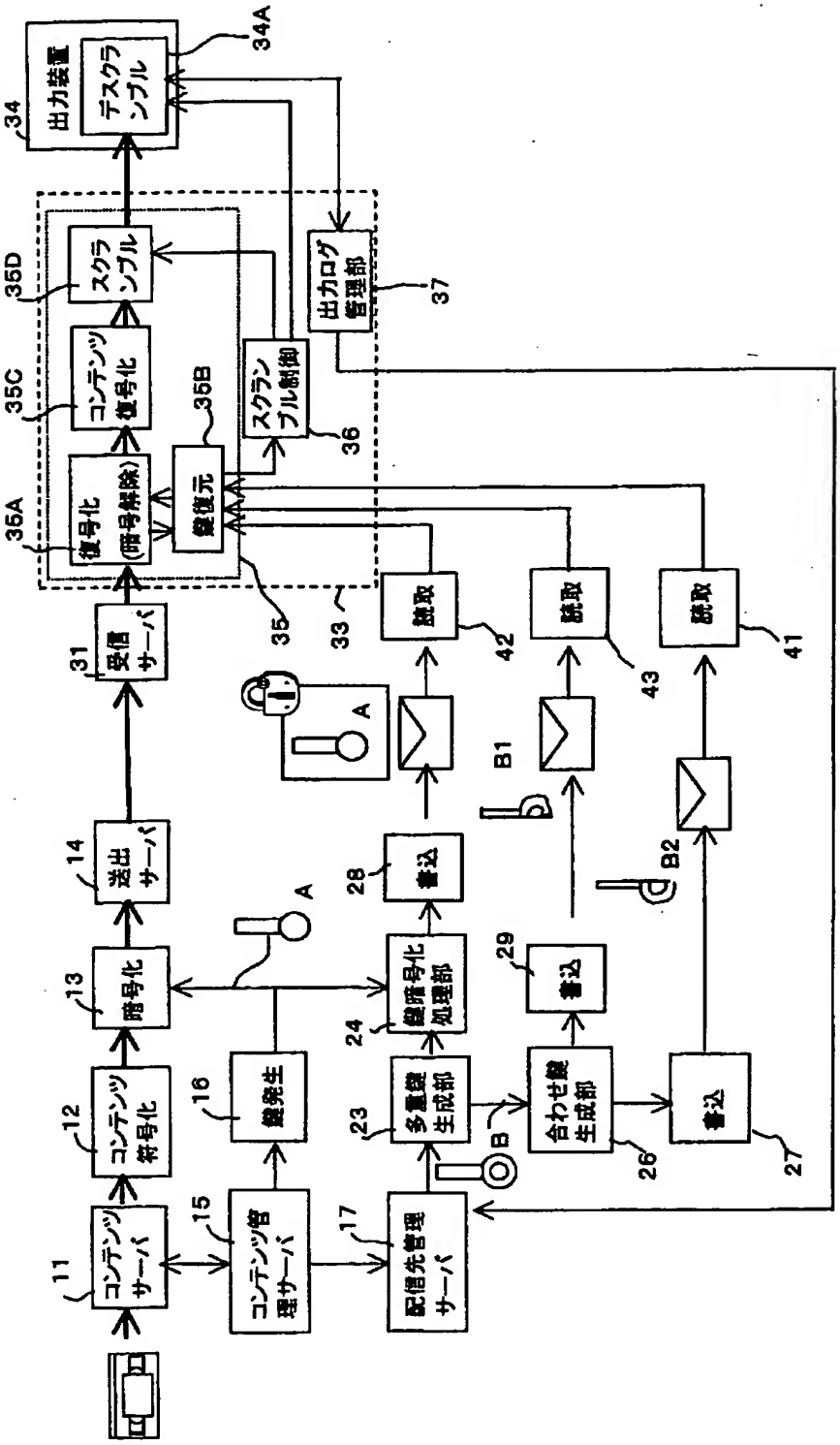
【図１５】


出力装置
34
デスクランブル
34A
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
15
多重鍵生成部
23
鍵暗号化処理部
24
配信先管理サーバ
17
書込
28
書込
25
読取
42
読取
40
A
A

【図１６】


出力装置
デスクラシブル
34
34A
スクラシブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
受信サーバ
31
35
33
A
B1
B2
送出サーバ
14
暗号化
13
コンテンツ符号化
12
鍵発生
16
鍵暗号化処理部
24
多重鍵生成部
23
合わせ鍵生成部
26
B
コンテンツサーバ
11
コンテンツ管理サーバ
15
配信先管理サーバ
17

【図１７】


出力装置
34
34A
デスクラシングル
スクラシングル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
コンテンツ管理サーバ
15
鍵発生
16
配信先管理サーバ
17
鍵情報暗号化処理部
24
多重鍵生成部
23
合わせ鍵生成部
26
書込
27
書込
28
書込
29
読取
42
読取
43
読取
41
A
B
B1
B2

【図１８】

	暗号鍵の発生者	符号化実行者	暗号化実行者	鍵情報の配信者	制作者側から見た暗号鍵の秘匿性	備考
1	制作者	制作者	制作者	制作者(2つ)	高	
2	同上	同上	同上	制作者(1つ)＋配信者(1つ)	高	配信者が暗号化された暗号鍵を入手
3	同上	同上	同上	配信者(2つ)	中	配信者が暗号鍵を入手して鍵情報を作成
4	同上	同上	配信者	制作者(2つ)	中	暗号鍵は配信者に通知される
5	同上	同上	同上	制作者(1つ)＋配信者(1つ)	中	同上
6	同上	同上	同上	配信者(2つ)	中	同上
7	同上	配信者	同上	制作者(2つ)	中	同上
8	同上	同上	同上	制作者(1つ)＋配信者(1つ)	中	同上
9	同上	同上	同上	配信者(2つ)	中	同上
10	配信者	制作者	制作者	制作者(2つ)	小	制作者が暗号鍵を入手して鍵情報を作成
11	同上	同上	同上	制作者(1つ)＋配信者(1つ)	小	同上
12	同上	同上	同上	配信者(2つ)	小	同上
13	同上	同上	配信者	制作者(2つ)	小	同上
14	同上	同上	同上	制作者(1つ)＋配信者(1つ)	小	同上
15	同上	同上	同上	配信者(2つ)	小	同上
16	同上	配信者	同上	制作者(2つ)	小	同上
17	同上	同上	同上	制作者(1つ)＋配信者(1つ)	小	同上
18	同上	同上	同上	配信者(2つ)	小	同上

【書類名】　要約書

【要約】

【課題】　不正行為の困難性とランニングコストの低減要求を両立する。

【解決手段】　復号サーバにおいて暗号処理の解除が許可されるとき、復号サーバ内で発生されたスクランブル鍵を用いて、暗号処理の解除されたディジタルコンテンツをスクランブル処理する。このようにスクランブル処理の施されたディジタルコンテンツを出力装置に与えることで、復号サーバと出力装置とを分離しても、当該伝送経路上で不正行為を行えないようにする。

【選択図】　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社